Guida per GuardDuty l'utente di Amazon

Amazon GuardDuty

Amazon GuardDuty: Guida per GuardDuty l'utente di Amazon

Table of Contents

Che cos'è GuardDuty? 1
Prezzi per GuardDuty 1
Accedendo GuardDuty 1
Nozioni di base 3
Prima di iniziare 3
Passaggio 1: abilitare Amazon GuardDuty 5
Fase 2: generare esiti di esempio ed esplorare le operazioni di base 7
Fase 3: configurare l'esportazione dei GuardDuty risultati in un bucket Amazon S3 8
Passaggio 4: configura la GuardDuty ricerca di avvisi tramite SNS 10
Passaggi successivi 13
Concetti e terminologia 15
GuardDuty attivazione delle funzionalità 19
Attivazioni delle funzionalità 19
GuardDuty Modifiche all'API 19
Attivazione delle funzionalità rispetto alle origini dati 20
Comprensione del funzionamento dell'attivazione delle funzionalità 20
Incorporazione delle modifiche all'attivazione delle funzionalità 21
Mappatura di `dataSources` su `features` 22
Origini dati fondamentali 25
AWS CloudTrail registri degli eventi 25
Come GuardDuty gestisce gli eventi AWS CloudTrail globali 26
AWS CloudTrail eventi gestionali 26
Log di flusso VPC 26
Log DNS 27
GuardDuty Protezione EKS 28
Funzionalità 28
Log di audit di Kubernetes 28
Monitoraggio dei log di audit EKS 29
Configurazione del monitoraggio dei log di audit EKS per un account autonomo 29
Configurazione del monitoraggio dei log di audit EKS in ambienti con più account 30
GuardDuty Protezione Lambda 38
Funzionalità 38
Monitoraggio delle attività di rete Lambda 38
Configurazione della Protezione Lambda 39

Configurazione della Protezione Lambda per un account autonomo 39
Configurazione della Protezione Lambda in ambienti multi-account 40
GuardDuty Protezione da malware 48
Funzionalità 50
Volume Elastic Block Storage (EBS) 50
Volumi EBS supportati 52
Modifica dell'ID della chiave KMS predefinita 52
Personalizzazioni nella protezione da malware 53
Impostazioni generali 53
Opzioni di scansione con tag definiti dall'utente 55
Tag GuardDutyExcluded globale 59
GuardDuty- scansione antimalware avviata 59
Configurazione della scansione antimalware avviata GuardDuty 61
Risultati che richiamano la scansione GuardDuty antimalware avviata 74
Scansione antimalware on demand 76
Come funziona la scansione antimalware on demand 76
Nozioni di base 78
Monitoraggio dello stato e del risultato delle scansioni malware 80
GuardDuty account di servizio 82
Quote di protezione da malware 84
GuardDuty Protezione RDS 89
Database supportati 89
Come la Protezione RDS utilizza il monitoraggio delle attività di accesso RDS 90
Configurazione della Protezione RDS per un account autonomo 91
Configurazione della Protezione RDS in ambienti con più account 91
Funzionalità 99
Monitoraggio delle attività di accesso RDS 99
Monitoraggio del runtime 100
Come funziona 101
Con istanze Amazon EC2 102
Con Fargate (solo Amazon ECS) 105
Con i cluster Amazon EKS 106
Dopo la configurazione del monitoraggio del runtime 106
Prova gratuita di 30 giorni 107
Sto usando il periodo di GuardDuty prova o non ho mai abilitato EKS Runtime Monitoring ... 107
Ho abilitato EKS Runtime Monitoring prima del lancio di Runtime Monitoring 108

Prerequisiti 109
Per l'istanza EC2 109
Per il cluster Fargate (solo ECS) 111
Per il cluster EKS 114
Concetti chiave: approcci alla gestione del GuardDuty Security Agent 116
Risorsa Fargate (solo Amazon ECS) - Approcci alla gestione degli agenti di sicurezza GuardDuty 117
Cluster Amazon EKS: approcci alla gestione degli agenti GuardDuty di sicurezza 118
Abilitazione del monitoraggio del runtime 122
Per account autonomo 123
Per ambienti con più account 123
Gestione degli agenti GuardDuty di sicurezza 128
Configurazione di EKS Runtime Monitoring (solo API) 235
Configurazione del monitoraggio del runtime EKS per un account autonomo 235
Configurazione del monitoraggio del runtime EKS per ambienti con più account 241
Migrazione da EKS Runtime Monitoring a Runtime Monitoring 282
Verifica dello stato della configurazione del monitoraggio di EKS Runtime 283
Disattivazione di EKS Runtime Monitoring dopo la migrazione a Runtime Monitoring 284
Pulizia delle risorse del Security Agent GuardDuty 285
Valutazione della copertura del runtime 287
Copertura per l'istanza Amazon EC2 288
Copertura per la risorsa Fargate (solo Amazon ECS) 297
Copertura per i cluster Amazon EKS 308
Domande frequenti (FAQ) 321
Configurazione del monitoraggio della CPU e della memoria 322
Tipi di eventi di runtime raccolti 323
Eventi di processo 323
Eventi del container 325
AWS Fargate (solo Amazon ECS) eventi relativi alle attività 325
Eventi pod di Kubernetes 326
Eventi DNS 326
Eventi aperti 327
Evento modulo di caricamento 327
Eventi mprotect 327
Eventi di montaggio 328
Eventi di collegamento 328

Eventi collegamento simbolico 328
Eventi dup 329
Evento mappa di memoria 329
Eventi socket 330
Connetti eventi 330
Eventi VM Readv processo 331
Eventi VM Writev processo 331
Eventi ptrace 332
Associa eventi 332
Ascolta gli eventi 333
Rinomina gli eventi 333
Imposta gli eventi UID 333
Eventi Chmod 334
Agente di hosting del repository Amazon ECR GuardDuty 334
Repository per GuardDuty agenti su cluster Amazon EKS 334
Repository per GuardDuty agente su AWS Fargate (solo Amazon ECS) 336
GuardDuty cronologia delle versioni degli agenti 339
GuardDuty Protezione S3 349
Come vengono utilizzati gli eventi relativi ai dati di S3 GuardDuty 349
Configurazione della Protezione S3 per un account autonomo 29
Per abilitare o disabilitare la Protezione S3 350
Configurazione della Protezione S3 in ambienti con più account 351
Funzionalità 359
AWS CloudTrail eventi relativi ai dati per S3 359
Comprensione degli esiti 360
Dettagli degli esiti 360
Panoramica degli esiti 361
Risorsa 362
Dettagli utente del database (DB) RDS 367
Dettagli relativi ai risultati di Runtime Mon 368
Dettagli della scansione dei volumi EBS 370
Dettagli degli esiti della protezione da malware 371
Azione 372
Attore o destinazione 374
Informazioni aggiuntive 375
Evidenza 375

Comportamento anomalo ... 376
Formato degli esiti di GuardDuty ... 381
Scopi delle minacce ... 382
Risultati di esempio ... 385
Generazione di risultati di esempio tramite la GuardDuty console o l'API ... 385
Generazione automatica di GuardDuty risultati comuni ... 386
Livelli di gravità dei GuardDuty risultati ... 388
GuardDuty ricerca dell'aggregazione ... 389
Individuazione e analisi dei risultati GuardDuty ... 390
Tipi di esiti ... 392
Tipi di esiti EC2 ... 392
Backdoor:EC2/C&CActivity.B ... 394
Backdoor:EC2/C&CActivity.B!DNS ... 395
Backdoor:EC2/DenialOfService.Dns ... 396
Backdoor:EC2/DenialOfService.Tcp ... 396
Backdoor:EC2/DenialOfService.Udp ... 397
Backdoor:EC2/DenialOfService.UdpOnTcpPorts ... 398
Backdoor:EC2/DenialOfService.UnusualProtocol ... 398
Backdoor:EC2/Spambot ... 399
Behavior:EC2/NetworkPortUnusual ... 399
Behavior:EC2/TrafficVolumeUnusual ... 400
CryptoCurrency:EC2/BitcoinTool.B ... 400
CryptoCurrency:EC2/BitcoinTool.B!DNS ... 401
DefenseEvasion:EC2/UnusualDNSResolver ... 402
DefenseEvasion:EC2/UnusualDoHActivity ... 402
DefenseEvasion:EC2/UnusualDoTActivity ... 403
Impact:EC2/AbusedDomainRequest.Reputation ... 403
Impact:EC2/BitcoinDomainRequest.Reputation ... 404
Impact:EC2/MaliciousDomainRequest.Reputation ... 405
Impact:EC2/PortSweep ... 406
Impact:EC2/SuspiciousDomainRequest.Reputation ... 406
Impact:EC2/WinRMBruteForce ... 407
Recon:EC2/PortProbeEMRUnprotectedPort ... 407
Recon:EC2/PortProbeUnprotectedPort ... 408
Recon:EC2/Portscan ... 409
Trojan:EC2/BlackholeTraffic ... 410

Trojan:EC2/BlackholeTraffic!DNS 410
Trojan:EC2/DGADomainRequest.B 411
Trojan:EC2/DGADomainRequest.C!DNS 412
Trojan:EC2/DNSDataExfiltration 413
Trojan:EC2/DriveBySourceTraffic!DNS 413
Trojan:EC2/DropPoint 414
Trojan:EC2/DropPoint!DNS 414
Trojan:EC2/PhishingDomainRequest!DNS 414
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom 415
UnauthorizedAccess:EC2/MetadataDNSRebind 416
UnauthorizedAccess:EC2/RDPBruteForce 417
UnauthorizedAccess:EC2/SSHBruteForce 417
UnauthorizedAccess:EC2/TorClient 419
UnauthorizedAccess:EC2/TorRelay 419
Tipi di esiti IAM 420
CredentialAccess:IAMUser/AnomalousBehavior 421
DefenseEvasion:IAMUser/AnomalousBehavior 422
Discovery:IAMUser/AnomalousBehavior 422
Exfiltration:IAMUser/AnomalousBehavior 423
Impact:IAMUser/AnomalousBehavior 424
InitialAccess:IAMUser/AnomalousBehavior 425
PenTest:IAMUser/KaliLinux 425
PenTest:IAMUser/ParrotLinux 426
PenTest:IAMUser/PentooLinux 426
Persistence:IAMUser/AnomalousBehavior 427
Policy:IAMUser/RootCredentialUsage 428
PrivilegeEscalation:IAMUser/AnomalousBehavior 428
Recon:IAMUser/MaliciousIPCaller 429
Recon:IAMUser/MaliciousIPCaller.Custom 430
Recon:IAMUser/TorIPCaller 430
Stealth:IAMUser/CloudTrailLoggingDisabled 431
Stealth:IAMUser/PasswordPolicyChange 431
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B 432
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS 432
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS 434
UnauthorizedAccess:IAMUser/MaliciousIPCaller 435

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom 436
UnauthorizedAccess:IAMUser/TorIPCaller 436
Tipi di esiti dei log di audit di Kubernetes 437
CredentialAccess:Kubernetes/MaliciousIPCaller 439
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom 440
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess 440
CredentialAccess:Kubernetes/TorIPCaller 441
DefenseEvasion:Kubernetes/MaliciousIPCaller 442
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom 442
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess 443
DefenseEvasion:Kubernetes/TorIPCaller 444
Discovery:Kubernetes/MaliciousIPCaller 445
Discovery:Kubernetes/MaliciousIPCaller.Custom 445
Discovery:Kubernetes/SuccessfulAnonymousAccess 446
Discovery:Kubernetes/TorIPCaller 447
Execution:Kubernetes/ExecInKubeSystemPod 447
Impact:Kubernetes/MaliciousIPCaller 448
Impact:Kubernetes/MaliciousIPCaller.Custom 449
Impact:Kubernetes/SuccessfulAnonymousAccess 449
Impact:Kubernetes/TorIPCaller 450
Persistence:Kubernetes/ContainerWithSensitiveMount 451
Persistence:Kubernetes/MaliciousIPCaller 451
Persistence:Kubernetes/MaliciousIPCaller.Custom 452
Persistence:Kubernetes/SuccessfulAnonymousAccess 453
Persistence:Kubernetes/TorIPCaller 453
Policy:Kubernetes/AdminAccessToDefaultServiceAccount 454
Policy:Kubernetes/AnonymousAccessGranted 455
Policy:Kubernetes/ExposedDashboard 455
Policy:Kubernetes/KubeflowDashboardExposed 456
PrivilegeEscalation:Kubernetes/PrivilegedContainer 456
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed 457
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated 458
Execution:Kubernetes/AnomalousBehavior.ExecInPod 459
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer 460

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount ... 461
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed ... 462
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated ... 463
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked ... 464
Tipi di esiti della Protezione Lambda ... 465
Backdoor:Lambda/C&CActivity.B ... 465
CryptoCurrency:Lambda/BitcoinTool.B ... 466
Trojan:Lambda/BlackholeTraffic ... 467
Trojan:Lambda/DropPoint ... 467
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom ... 468
UnauthorizedAccess:Lambda/TorClient ... 468
UnauthorizedAccess:Lambda/TorRelay ... 469
Tipi di esiti della protezione da malware ... 469
Execution:EC2/MaliciousFile ... 470
Execution:ECS/MaliciousFile ... 471
Execution:Kubernetes/MaliciousFile ... 471
Execution:Container/MaliciousFile ... 471
Execution:EC2/SuspiciousFile ... 472
Execution:ECS/SuspiciousFile ... 472
Execution:Kubernetes/SuspiciousFile ... 473
Execution:Container/SuspiciousFile ... 474
Tipi di esiti della Protezione RDS ... 474
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin ... 475
CredentialAccess:RDS/AnomalousBehavior.FailedLogin ... 476
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce ... 477
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin ... 478
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin ... 479
Discovery:RDS/MaliciousIPCaller ... 479
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin ... 480
CredentialAccess:RDS/TorIPCaller.FailedLogin ... 481
Discovery:RDS/TorIPCaller ... 481
Tipi di risultati del monitoraggio del runtime ... 482
CryptoCurrency:Runtime/BitcoinTool.B ... 484
Backdoor:Runtime/C&CActivity.B ... 484
UnauthorizedAccess:Runtime/TorRelay ... 485

UnauthorizedAccess:Runtime/TorClient 486
Trojan:Runtime/BlackholeTraffic 487
Trojan:Runtime/DropPoint 487
CryptoCurrency:Runtime/BitcoinTool.B!DNS 488
Backdoor:Runtime/C&CActivity.B!DNS 489
Trojan:Runtime/BlackholeTraffic!DNS 490
Trojan:Runtime/DropPoint!DNS 491
Trojan:Runtime/DGADomainRequest.C!DNS 491
Trojan:Runtime/DriveBySourceTraffic!DNS 492
Trojan:Runtime/PhishingDomainRequest!DNS 493
Impact:Runtime/AbusedDomainRequest.Reputation 493
Impact:Runtime/BitcoinDomainRequest.Reputation 494
Impact:Runtime/MaliciousDomainRequest.Reputation 495
Impact:Runtime/SuspiciousDomainRequest.Reputation 496
UnauthorizedAccess:Runtime/MetadataDNSRebind 497
Execution:Runtime/NewBinaryExecuted 498
PrivilegeEscalation:Runtime/DockerSocketAccessed 499
PrivilegeEscalation:Runtime/RuncContainerEscape 499
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified 500
DefenseEvasion:Runtime/ProcessInjection.Proc 501
DefenseEvasion:Runtime/ProcessInjection.Ptrace 502
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite 502
Execution:Runtime/ReverseShell 503
DefenseEvasion:Runtime/FilelessExecution 503
Impact:Runtime/CryptoMinerExecuted 504
Execution:Runtime/NewLibraryLoaded 505
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory 505
PrivilegeEscalation:Runtime/UserfaultfdUsage 506
Execution:Runtime/SuspiciousTool 507
Execution:Runtime/SuspiciousCommand 507
DefenseEvasion:Runtime/SuspiciousCommand 508
DefenseEvasion:Runtime/PtraceAntiDebugging 509
Execution:Runtime/MaliciousFileExecuted 510
Tipi di esiti S3 510
Discovery:S3/AnomalousBehavior 512
Discovery:S3/MaliciousIPCaller 512

Discovery:S3/MaliciousIPCaller.Custom 513
Discovery:S3/TorIPCaller 513
Exfiltration:S3/AnomalousBehavior 514
Exfiltration:S3/MaliciousIPCaller 515
Impact:S3/AnomalousBehavior.Delete 515
Impact:S3/AnomalousBehavior.Permission 516
Impact:S3/AnomalousBehavior.Write 517
Impact:S3/MaliciousIPCaller 518
PenTest:S3/KaliLinux 518
PenTest:S3/ParrotLinux 519
PenTest:S3/PentooLinux 519
Policy:S3/AccountBlockPublicAccessDisabled 520
Policy:S3/BucketAnonymousAccessGranted 521
Policy:S3/BucketBlockPublicAccessDisabled 522
Policy:S3/BucketPublicAccessGranted 522
Stealth:S3/ServerAccessLoggingDisabled 523
UnauthorizedAccess:S3/MaliciousIPCaller.Custom 524
UnauthorizedAccess:S3/TorIPCaller 524
Tipi di esiti ritirati 525
Exfiltration:S3/ObjectRead.Unusual 526
Impact:S3/PermissionsModification.Unusual 526
Impact:S3/ObjectDelete.Unusual 527
Discovery:S3/BucketEnumeration.Unusual 528
Persistence:IAMUser/NetworkPermissions 528
Persistence:IAMUser/ResourcePermissions 529
Persistence:IAMUser/UserPermissions 530
PrivilegeEscalation:IAMUser/AdministrativePermissions 531
Recon:IAMUser/NetworkPermissions 532
Recon:IAMUser/ResourcePermissions 532
Recon:IAMUser/UserPermissions 533
ResourceConsumption:IAMUser/ComputeResources 534
Stealth:IAMUser/LoggingConfigurationModified 535
UnauthorizedAccess:IAMUser/ConsoleLogin 535
UnauthorizedAccess:EC2/TorIPCaller 536
Backdoor:EC2/XORDDOS 536
Behavior:IAMUser/InstanceLaunchUnusual 537

CryptoCurrency:EC2/BitcoinTool.A 537
UnauthorizedAccess:IAMUser/UnusualASNCaller 538
Esiti per tipo di risorsa 538
Tabella degli esiti 538
Gestione dei GuardDuty risultati 565
Riepilogo 566
Accesso al pannello di Riepilogo 566
Comprensione del pannello di Riepilogo 567
Feedback sul pannello di Riepilogo 570
Filtro dei risultati 570
Creazione di filtri nella console GuardDuty 571
Attributi del filtro 572
Regole di eliminazione 578
..... 578
Casi d'uso comuni per le regole di eliminazione ed esempi 579
Per creare regole di soppressione in GuardDuty 582
..... 584
Elenchi di indirizzi IP affidabili ed elenchi minacce 586
Formati di elenco 587
Autorizzazioni necessarie per caricare elenchi di indirizzi IP affidabili ed elenchi minacce 590
Utilizzo della crittografia lato server per elenchi di indirizzi IP affidabili ed elenchi minacce ... 591
Aggiunta e attivazione di un elenco di indirizzi IP affidabili o di IP delle minacce 592
Aggiornamento di elenchi di indirizzi IP affidabili e di elenchi minacce 594
Disattivazione o eliminazione di un elenco di indirizzi IP affidabili o un elenco minacce 596
Esportazione degli esiti 597
Considerazioni 598
Fase 1 — Autorizzazioni necessarie per esportare i risultati 599
Fase 2: allegare la policy alla chiave KMS 599
Fase 3: Allegare la policy al bucket Amazon S3 601
Fase 4 - Esportazione dei risultati in un bucket S3 (console) 605
Fase 5 — Frequenza di aggiornamento dell'esportazione 606
Automatizzazione delle risposte con Events CloudWatch 607
CloudWatch Frequenza di notifica degli eventi per GuardDuty 608
CloudWatch formato di evento per GuardDuty 609
Creazione di una regola CloudWatch Events per notificare GuardDuty i risultati (console) ... 610
Creazione di una regola CloudWatch Events e di un target per GuardDuty (CLI) 616

CloudWatch Eventi per ambienti GuardDuty con più account ... 618
Comprensione dei CloudWatch log e dei motivi per cui le risorse vengono ignorate ... 619
Controllo dei GuardDuty log in Malware CloudWatch Protection ... 619
GuardDuty Conservazione dei log di Malware Protection ... 621
Motivi per cui una risorsa viene ignorata ... 621
Segnalazione di falsi positivi nella protezione da malware ... 627
Invio di un file falso positivo ... 627
Correzioni degli esiti ... 628
Correzione di un'istanza Amazon EC2 potenzialmente compromessa ... 628
Riparazione di un bucket S3 potenzialmente compromesso ... 630
Consigli basati su esigenze specifiche di accesso ai bucket S3 ... 631
Riparazione di un cluster ECS potenzialmente compromesso ... 632
Riparazione delle credenziali potenzialmente compromesse AWS ... 633
Riparazione di un contenitore autonomo potenzialmente compromesso ... 634
Correzione degli esiti del monitoraggio dei log di audit EKS ... 635
Potenziali problemi di configurazione ... 636
Riparare gli utenti Kubernetes potenzialmente compromessi ... 636
Riparazione dei pod Kubernetes potenzialmente compromessi ... 639
Riparazione delle immagini dei container potenzialmente compromesse ... 641
Riparazione dei nodi Kubernetes potenzialmente compromessi ... 641
Correzione dei risultati del Runtime Monitoring ... 642
Correzione delle immagini del container compromesse ... 644
Ripristino di un database potenzialmente compromesso ... 644
Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti ... 645
Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti ... 646
Correzione di credenziali potenzialmente compromesse ... 647
Limita l'accesso alla rete ... 647
Correzione di una funzione Lambda potenzialmente compromessa ... 648
Gestione di più account ... 650
Gestione di più account con AWS Organizations ... 650
Gestione di più account tramite invito ... 650
GuardDuty relazioni tra account amministratore e account membro ... 651
Gestione degli account con AWS Organizations ... 654
Considerazioni e raccomandazioni ... 655

Autorizzazioni necessarie per designare un account amministratore delegato GuardDuty 657
Designazione di un account GuardDuty amministratore delegato e gestione dei membri tramite la console 658
Designazione di un account GuardDuty amministratore GuardDuty delegato e gestione dei membri utilizzando l'API 663
Mantenere la propria organizzazione all'interno GuardDuty 667
Modifica dell'account amministratore delegato GuardDuty 668
Gestione degli account tramite invito 670
Aggiunta e gestione degli account tramite invito 671
Consolidamento degli account di GuardDuty amministratore in un unico account di amministratore delegato GuardDuty dell'organizzazione 676
Abilita più account GuardDuty contemporaneamente 678
Stima del costo 681
Comprendere come calcola i costi di utilizzo GuardDuty 681
Monitoraggio del runtime: in che modo i log di flusso VPC delle istanze EC2 influiscono sui costi di utilizzo 682
Come GuardDuty stima i costi di utilizzo per CloudTrail gli eventi 682
Revisione delle statistiche GuardDuty di utilizzo 683
Sicurezza 685
Protezione dei dati 685
Crittografia dei dati a riposo 686
Crittografia in transito 687
Rifiuto esplicito all'utilizzo dei dati volto al miglioramento del servizio 687
Registrazione con CloudTrail 688
GuardDuty informazioni in CloudTrail 689
GuardDuty eventi del piano di controllo in CloudTrail 690
GuardDuty eventi relativi ai dati in CloudTrail 690
Esempio: voci dei file di registro GuardDuty 691
Identity and Access Management 694
Destinatari 694
Autenticazione con identità 695
Gestione dell'accesso con policy 699
Come GuardDuty funziona Amazon con IAM 701
Esempi di policy basate su identità 708
Uso di ruoli collegati ai servizi 717
Risoluzione dei problemi 737

AWS politiche gestite ... 739
Convalida della conformità ... 748
Resilienza ... 750
Sicurezza dell'infrastruttura ... 750
Integrazioni GuardDuty ... 751
Integrazione di GuardDuty con AWS Security Hub ... 751
Integrazione di GuardDuty con Amazon Detective ... 751
Integrazione di Security Hub ... 751
In che modo Amazon GuardDuty invia i risultati a AWS Security Hub ... 752
Visualizzazione dei risultati GuardDuty in AWS Security Hub ... 753
Abilitazione e configurazione dell'integrazione ... 768
Interruzione dell'invio degli esiti a Security Hub ... 769
Integrazione di Detective ... 769
Abilitazione dell'integrazione ... 769
Passaggio ad Amazon Detective da un esito di GuardDuty ... 770
Utilizzo dell'integrazione con un ambiente multi-account GuardDuty ... 770
Sospensione o disabilitazione ... 772
GuardDuty annunci ... 773
Formato dei messaggi Amazon SNS ... 779
Quote ... 783
Risoluzione dei problemi ... 787
Problemi generali in GuardDuty ... 787
Ricevo un errore di accesso durante l'esportazione dei GuardDuty risultati. Come posso risolvere questo problema? ... 787
Problemi di protezione da malware ... 788
All'avvio di una scansione antimalware on demand ricevo un messaggio di un errore che segnala la mancanza delle autorizzazioni richieste. ... 788
Ricevo un errore `iam:GetRole` mentre utilizzo la protezione da malware. ... 788
Sono un account GuardDuty amministratore che deve abilitare la scansione antimalware GuardDuty avviata dall'utente, ma non utilizza AWS Managed Policy: to manage. AmazonGuardDutyFullAccess GuardDuty ... 788
Problemi di monitoraggio del runtime ... 788
Il mio AWS Step Functions flusso di lavoro non funziona in modo imprevisto ... 788
Risoluzione dell'errore di esaurimento della memoria ... 789
Gestione dei problemi relativi a più account ... 790

Desidero gestire più account ma non dispongo dell'autorizzazione di AWS Organizations gestione richiesta. 790
Altre questioni relative alla risoluzione dei problemi 790
Regioni ed endpoint 791
Disponibilità di funzionalità specifiche per ogni regione 791
Operazioni e parametri legacy 793
Cronologia dei documenti 795
Aggiornamenti precedenti 847
..... dcccxlviii

Che cos'è Amazon GuardDuty?

Amazon GuardDuty è un servizio di monitoraggio della sicurezza che analizza ed elabora eventi di AWS CloudTrail gestioneOrigini dati fondamentali, log di AWS CloudTrail eventi, log di flusso VPC (da istanze Amazon EC2) e log DNS. Elabora inoltre funzionalità come i log di audit di Kubernetes, le attività di accesso RDS, i log S3, i volumi EBS, il monitoraggio del runtime e i log delle attività di rete Lambda. Utilizza feed di intelligence sulle minacce, come elenchi di domini e di IP dannosi nonché il machine learning per identificare attività non previste, potenzialmente non autorizzate e dannose all'interno del tuo ambiente AWS. Ciò può includere problemi come l'escalation di privilegi, l'utilizzo di credenziali esposte o la comunicazione con indirizzi IP o domini dannosi, la presenza di malware sulle istanze Amazon EC2 e sui carichi di lavoro di un container o il rilevamento di schemi insoliti relativi agli eventi di accesso sul tuo database. Ad esempio, è in GuardDuty grado di rilevare istanze EC2 compromesse e carichi di lavoro in container che contengono malware o estraggono bitcoin. Monitora inoltra il comportamento di accesso all'account AWS alla ricerca di segni di compromissione come implementazioni dell'infrastruttura non autorizzate, ad esempio istanze implementate in una regione che non era mai stata utilizzata in precedenza, o chiamate API insolite, ad esempio la modifica di una policy delle password volta a ridurre l'efficacia delle password.

GuardDuty ti informa sullo stato del tuo AWS ambiente producendo risultati di sicurezza che puoi visualizzare nella GuardDuty console o tramite Amazon EventBridge. GuardDuty fornisce inoltre supporto per esportare i risultati in un bucket Amazon Simple Storage Service (S3) e integrarli con altri servizi come Detective. AWS Security Hub

Prezzi per GuardDuty

Per informazioni sui GuardDuty prezzi, consulta la pagina GuardDuty dei prezzi di Amazon.

Accedendo GuardDuty

Puoi lavorare con GuardDuty in uno dei seguenti modi:

GuardDuty console

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

La console è un'interfaccia basata su browser che consente l'accesso a GuardDuty e il suo utilizzo. La GuardDuty console fornisce l'accesso all' GuardDuty account, ai dati e alle risorse.

Strumenti a riga di comando AWS

Con gli strumenti da riga di AWS comando, è possibile impartire comandi dalla riga di comando del sistema per eseguire GuardDuty attività e AWS attività. Gli strumenti a riga di comando sono utili per creare script che eseguono le attività.

Per informazioni sull'installazione e l'utilizzo della AWS CLI, consulta la Guida per l'utente della AWS Command Line Interface. Per visualizzare i AWS CLI comandi disponibili per GuardDuty, consulta il riferimento ai comandi CLI.

GuardDuty API HTTPS

Puoi GuardDuty accedervi in modo AWS programmatico utilizzando l'API GuardDuty HTTPS, che consente di inviare richieste HTTPS direttamente al servizio. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di GuardDuty .

AWS SDK

AWS fornisce kit SDK costituiti da librerie e codice di esempio per vari linguaggi e piattaforme di programmazione (Java, Python, Ruby, .NET, iOS, Android e così via). Gli SDK rappresentano un sistema molto comodo per creare un accesso programmatico a GuardDuty. Per ulteriori informazioni sugli SDK AWS, inclusi i dettagli su come scaricarli e installarli, consulta Strumenti per Amazon Web Services.

Guida introduttiva con GuardDuty

Questo tutorial fornisce un'introduzione pratica a. GuardDuty I requisiti minimi per l'abilitazione GuardDuty come account autonomo o come GuardDuty amministratore AWS Organizations sono descritti nella Fase 1. I passaggi da 2 a 5 riguardano l'utilizzo di funzionalità aggiuntive consigliate da GuardDuty per ottenere il massimo dai risultati.

Argomenti

- Prima di iniziare
- Passaggio 1: abilitare Amazon GuardDuty
- Fase 2: generare esiti di esempio ed esplorare le operazioni di base
- Fase 3: configurare l'esportazione dei GuardDuty risultati in un bucket Amazon S3
- Passaggio 4: configura la GuardDuty ricerca di avvisi tramite SNS
- Passaggi successivi

Prima di iniziare

GuardDuty è un servizio di rilevamento delle minacce che monitora Origini dati fondamentali log di AWS CloudTrail eventi, eventi di AWS CloudTrail gestione, Amazon VPC Flow Logs e log DNS. GuardDuty analizza anche le funzionalità associate ai suoi tipi di protezione solo se le abiliti separatamente. Le funzionalità includono i log di audit di Kubernetes, le attività di accesso RDS, i log S3, i volumi EBS, il monitoraggio del runtime e i log delle attività di rete Lambda. L'utilizzo di queste fonti di dati e funzionalità (se abilitate), GuardDuty genera risultati di sicurezza per il tuo account.

Dopo l'attivazione GuardDuty, inizia a monitorare l'ambiente. Puoi disattivarlo GuardDuty per qualsiasi account in qualsiasi regione, in qualsiasi momento. Ciò GuardDuty impedirà l'elaborazione delle fonti di dati di base e di tutte le funzionalità che sono state abilitate separatamente.

Non è necessario abilitare esplicitamente le Origini dati fondamentali. Amazon GuardDuty estrae flussi di dati indipendenti direttamente da tali servizi. Per un nuovo GuardDuty account, tutti i tipi di protezione disponibili supportati in un Regione AWS sono abilitati e inclusi nel periodo di prova gratuito di 30 giorni per impostazione predefinita. È possibile disattivarne alcuni o tutti. Se sei un GuardDuty cliente esistente, puoi scegliere di abilitare uno o tutti i piani di protezione disponibili nel tuo Regione AWS. Per ulteriori informazioni, consulta Funzionalità associate a ciascun tipo di protezione in GuardDuty.

Durante l'attivazione GuardDuty, considera i seguenti elementi:

- GuardDuty è un servizio regionale, il che significa che tutte le procedure di configurazione seguite in questa pagina devono essere ripetute in ogni regione con cui si desidera monitorare GuardDuty.

  Ti consigliamo vivamente di abilitarlo GuardDuty in tutte le AWS regioni supportate. Ciò consente di GuardDuty generare informazioni su attività non autorizzate o insolite anche nelle Regioni che non utilizzi attivamente. Ciò consente inoltre di GuardDuty monitorare AWS CloudTrail gli eventi per AWS servizi globali come IAM. Se non GuardDuty è abilitato in tutte le regioni supportate, la sua capacità di rilevare attività che coinvolgono servizi globali è ridotta. Per un elenco completo delle regioni in cui GuardDuty è disponibile, consultaRegioni ed endpoint.
- Qualsiasi utente con privilegi di amministratore in un AWS account può abilitare GuardDuty, tuttavia, seguendo la migliore pratica di sicurezza del privilegio minimo, si consiglia di creare un ruolo, un utente o un gruppo IAM da gestire GuardDuty in modo specifico. Per informazioni sulle autorizzazioni necessarie per l'attivazione, vedere. GuardDuty Autorizzazioni necessarie per abilitare GuardDuty
- Quando si abilita GuardDuty per la prima volta in qualsiasi regione Regione AWS, per impostazione predefinita, vengono attivati anche tutti i tipi di protezione disponibili supportati in quella regione, inclusa la protezione da malware. GuardDuty crea un ruolo collegato al servizio per il tuo account chiamato. `AWSServiceRoleForAmazonGuardDuty` Questo ruolo include le autorizzazioni e le politiche di fiducia che consentono GuardDuty di utilizzare e analizzare gli eventi direttamente dal Origini dati fondamentali per generare risultati di sicurezza. La protezione da malware crea un altro ruolo collegato ai servizi per il tuo account chiamato `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Questo ruolo include le autorizzazioni e le politiche di fiducia che consentono a Malware Protection di eseguire scansioni senza agenti per rilevare il malware nell'account. GuardDuty Consente di GuardDuty creare un'istantanea del volume EBS nel tuo account e condividerla con l'account del servizio. GuardDuty Per ulteriori informazioni, consulta Autorizzazioni di ruolo collegate al servizio per GuardDuty. Per ulteriori informazioni sui ruoli collegati ai servizi, consulta Utilizzo di ruoli collegati ai servizi.

- Quando lo attivi GuardDuty per la prima volta in qualsiasi regione, il tuo AWS account viene automaticamente registrato a una prova GuardDuty gratuita di 30 giorni per quella regione.

Passaggio 1: abilitare Amazon GuardDuty

Il primo passaggio per utilizzarlo GuardDuty è abilitarlo nel tuo account. Una volta abilitato, GuardDuty inizierà immediatamente a monitorare le minacce alla sicurezza nella regione corrente.

Se desideri gestire GuardDuty i risultati di altri account all'interno della tua organizzazione in qualità di GuardDuty amministratore, devi aggiungere e abilitare anche GuardDuty gli account dei membri. Scegli un'opzione per scoprire come attivarla GuardDuty per il tuo ambiente.

Standalone account environment

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/
2. Seleziona Inizia.
3. Scegli Abilita GuardDuty.

Multi-account environment

> **Important**
>
> Come prerequisiti per questo processo, devi far parte della stessa organizzazione di tutti gli account che desideri gestire e avere accesso all'account di AWS Organizations gestione per delegare un amministratore GuardDuty all'interno dell'organizzazione. Potrebbero essere necessarie autorizzazioni aggiuntive per delegare un amministratore. Per maggiori informazioni, consulta Autorizzazioni necessarie per designare un account amministratore delegato GuardDuty .

Per designare un account amministratore delegato GuardDuty

1. Apri la AWS Organizations console all'indirizzo https://console.aws.amazon.com/organizations/, utilizzando l'account di gestione.
2. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   È GuardDuty già abilitata nel tuo account?

   - Se non GuardDuty è già abilitato, puoi selezionare Inizia e quindi designare un amministratore GuardDuty delegato nella pagina Benvenuto GuardDuty.

- Se GuardDuty è abilitato, puoi designare un amministratore GuardDuty delegato nella pagina Impostazioni.

3. Inserisci l'ID dell'account a dodici cifre dell' AWS account che desideri designare come amministratore delegato dell'organizzazione e scegli GuardDuty Delegato.

> **Note**
>
> Se non GuardDuty è già abilitato, la designazione di un amministratore delegato lo abiliterà per quell'account nella regione corrente. GuardDuty

Per aggiungere account membri

Questa procedura prevede l'aggiunta di account membri a un account amministratore GuardDuty delegato tramite. AWS Organizations In alternativa è possibile aggiungere membri tramite invito. Per ulteriori informazioni su entrambi i metodi di associazione dei membri in GuardDuty, consulta. Gestione di più account in Amazon GuardDuty

1. Accedere all'account amministratore delegato
2. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
3. Nel riquadro di navigazione, scegliere Settings (Impostazioni), quindi Accounts (Account).

   Nella tabella account vengono visualizzati tutti gli account dell'organizzazione.
4. Scegli gli account che desideri aggiungere come membri selezionando la casella accanto all'ID account. Quindi, dal menu Operazione seleziona Aggiungi membro.

> **Tip**
>
> Puoi automatizzare l'aggiunta di nuovi account come membri attivando la funzionalità di Abilitazione automatica, che però si applica solo agli account che entrano a far parte dell'organizzazione dopo l'abilitazione della funzionalità.

Fase 2: generare esiti di esempio ed esplorare le operazioni di base

Quando GuardDuty rileva un problema di sicurezza, genera un risultato. Un GuardDuty risultato è un set di dati contenente dettagli relativi a quell'unico problema di sicurezza. I dettagli dell'esito possono essere utilizzati per indagare sul problema.

GuardDuty supporta la generazione di risultati di esempio con valori segnaposto, che possono essere utilizzati per testare GuardDuty la funzionalità e acquisire familiarità con i risultati prima di dover rispondere a un problema di sicurezza reale scoperto da. GuardDuty Segui la guida riportata di seguito per generare risultati di esempio per ogni tipo di risultato disponibile. Per ulteriori modi per generare risultati di esempio GuardDuty, inclusa la generazione di un evento di sicurezza simulato all'interno del tuo account, consulta. Risultati di esempio

Per creare ed esplorare gli esiti di esempio

1. Nel pannello di navigazione scegli Impostazioni.
2. Nella pagina Settings (Impostazioni), in Sample findings (Risultati di esempio), selezionare Generate sample findings (Genera risultati di esempio).
3. Nel riquadro di navigazione, scegli Riepilogo per visualizzare le informazioni dettagliate sui risultati generati nel tuo AWS ambiente. Per ulteriori informazioni sui componenti del pannello di Riepilogo, consulta Pannello di riepilogo.
4. Nel riquadro di navigazione, seleziona Esiti. Gli esiti di esempio vengono visualizzati nella pagina Risultati attuali con il prefisso [ESEMPIO].
5. Seleziona un esito dall'elenco per visualizzarne i dettagli.

    - È possibile esaminare i diversi campi informativi disponibili nel riquadro dei dettagli degli esiti. Diversi tipi di esiti possono avere campi diversi. Per ulteriori informazioni sui campi disponibili in tutti i tipi di esiti, consulta Dettagli degli esiti. Dal riquadro dei dettagli, puoi effettuare le operazioni seguenti:

        - Seleziona l'ID risultato nella parte superiore del riquadro per aprire i dettagli JSON completi dell'esito. Il file JSON completo può anche essere scaricato da questo pannello. Il file contiene alcune informazioni aggiuntive non incluse nella visualizzazione della console ed è in formato JSON, che può essere acquisito da altri strumenti e servizi.
        - Visualizza la sezione Risorsa interessata. Se si tratta di una scoperta reale, le informazioni qui riportate ti aiuteranno a identificare una risorsa nel tuo account che

dovrebbe essere analizzata e includeranno collegamenti a risorse utili. AWS Management Console

- Seleziona l'icona che raffigura una lente di ingrandimento con i simboli "+" o "-" per creare un filtro inclusivo o esclusivo per il dettaglio selezionato. Per ulteriori informazioni sui filtri per gli esiti, consulta Filtro dei risultati.

6. Archiviare tutti gli esiti di esempio

   a. Seleziona tutti gli esiti tramite la casella di controllo nella parte superiore dell'elenco.

   b. Deseleziona gli esiti che desideri conservare.

   c. Seleziona il menu Operazioni, quindi scegli Archivia per nascondere gli esiti di esempio.

> **Note**
>
> Per visualizzare gli esiti archiviati, seleziona Correnti, quindi Archiviati per cambiare la visualizzazione degli esiti.

Fase 3: configurare l'esportazione dei GuardDuty risultati in un bucket Amazon S3

GuardDuty consiglia di configurare le impostazioni per esportare i risultati perché consente di esportare i risultati in un bucket S3 per l'archiviazione a tempo indeterminato oltre il periodo di conservazione di 90 giorni. GuardDuty Ciò consente di tenere traccia dei risultati o tenere traccia dei problemi all'interno del proprio ambiente nel tempo. AWS Il processo descritto di seguito ti guida nella configurazione di un nuovo bucket S3 e nella creazione di una nuova chiave KMS per crittografare gli esiti dall'interno della console. Per ulteriori informazioni su questo argomento, ad esempio su come utilizzare il tuo bucket esistente o il bucket di un altro account, consulta Esportazione degli esiti.

Per configurare l'opzione di esportazione degli esiti in S3

1. Per crittografare i risultati, avrai bisogno di una chiave KMS con una politica che GuardDuty consenta di utilizzare tale chiave per la crittografia. Le fasi seguenti ti aiuteranno a creare una nuova chiave KMS. Se utilizzi una chiave KMS di un altro account, devi applicare la politica delle chiavi accedendo al proprietario della Account AWS chiave. La regione della chiave KMS e del bucket S3 deve essere la stessa. Tuttavia, puoi utilizzare lo stesso bucket e la stessa coppia di chiavi per ogni regione da cui desideri esportare gli esiti.

a. Apri la AWS KMS console all'indirizzo https://console.aws.amazon.com/kms.

b. Per modificare la Regione AWS, usa il selettore della regione nell'angolo superiore destro della pagina.

c. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.

d. Scegliere Create key (Crea chiave).

e. Scegli Simmetrico in Tipo di chiave, quindi Successivo.

> **Note**
>
> Per consultare in maggiore dettaglio le fasi per la creazione di una chiave KMS, consulta Creazione di chiavi nella Guida per gli sviluppatori di AWS Key Management Service .

f. Fornisci un Alias per la tua chiave, quindi scegli Successivo.

g. Scegli Successivo, quindi nuovamente Successivo per accettare le autorizzazioni di amministrazione e utilizzo predefinite.

h. Dopo aver effettuato la Revisione della configurazione, scegli Fine per creare la chiave.

i. Nella pagina Chiavi gestite dal cliente, scegli l'alias della chiave.

j. Nella scheda Policy della chiave, scegli Passa alla visualizzazione della policy.

k. Scegli Modifica e aggiungi la seguente politica chiave alla tua chiave KMS, garantendo GuardDuty l'accesso alla tua chiave. Questa dichiarazione consente di GuardDuty utilizzare solo la chiave a cui aggiungi questa politica. Quando modifichi la policy della chiave, assicurati che la sintassi JSON sia valida. Se aggiungi l'istruzione prima dell'istruzione finale, devi aggiungere una virgola dopo la parentesi di chiusura.

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "arn:aws:kms:Region1:444455556666:key/KMSKeyId",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333",
```

```
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:111122223333:detector/SourceDetectorID"
        }
    }
}
```

Sostituisci *Region1* con la regione della tua chiave KMS. Sostituisci *444455556666* con Account AWS quella che possiede la chiave KMS. Sostituisci *KMS KeyId* con l'ID della chiave KMS che hai scelto per la crittografia. Per identificare tutti questi valori: regione e ID chiave, visualizza l'ARN della tua chiave KMS. Account AWS Per individuare l'ARN della chiave, consulta Individuazione dell'ID e dell'ARN della chiave.

Allo stesso modo, sostituisci *111122223333* con il codice dell' Account AWS account. GuardDuty Sostituisci *Region2* con la regione dell'account. GuardDuty *Sostituisci SourceDetectorID con l'ID del rilevatore dell' GuardDuty account per Region2.*

Per trovare il codice relativo `detectorId` al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

l. Selezionare Salva.

2. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
3. Nel pannello di navigazione scegli Impostazioni.
4. Nella sezione Opzioni di esportazione dei risultati, scegli Configura ora.
5. Scegli Nuovo bucket. Fornisci un nome univoco per il bucket S3.
6. (Facoltativo) puoi testare le nuove impostazioni di esportazione generando esiti di esempio. Nel pannello di navigazione scegli Impostazioni.
7. Nella pagina Risultati di esempio, scegli Genera risultati di esempio. I nuovi risultati di esempio verranno visualizzati come voci nel bucket S3 creato da entro un massimo GuardDuty di cinque minuti.

Passaggio 4: configura la GuardDuty ricerca di avvisi tramite SNS

GuardDuty si integra con Amazon EventBridge, che può essere utilizzato per inviare i dati dei risultati ad altre applicazioni e servizi per l'elaborazione. Con EventBridge puoi utilizzare GuardDuty i risultati per avviare risposte automatiche ai tuoi risultati collegando gli eventi di ricerca a obiettivi come AWS

Lambda funzioni, automazione di Amazon EC2 Systems Manager, Amazon Simple Notification Service (SNS) e altro ancora.

In questo esempio creerai un argomento SNS come obiettivo di una EventBridge regola, quindi lo utilizzerai EventBridge per creare una regola da cui acquisire i dati dei risultati. GuardDuty La regola risultante inoltra i dettagli degli esiti a un indirizzo e-mail. Per scoprire come inviare gli esiti a Slack o Amazon Chime e come modificare i tipi di esiti per cui vengono inviati gli avvisi, consulta Impostare un argomento Amazon SNS e un endpoint.

Per creare un argomento SNS per gli avvisi sugli esiti

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nel pannello di navigazione, scegli Topics (Argomenti).
3. Seleziona Create Topic (Crea argomento).
4. Per Tipo, seleziona Standard.
5. Per Nome, immetti **`GuardDuty`**.
6. Seleziona Create Topic (Crea argomento). Verranno aperti i dettagli dell'argomento per il nuovo argomento.
7. Nella sezione Subscriptions (Sottoscrizioni) scegliere Create subscription (Crea sottoscrizione).
8. Per Protocollo, scegli E-mail.
9. Per Endpoint, inserisci l'indirizzo e-mail a cui desideri che vengano inviate le notifiche.
10. Scegli Crea sottoscrizione.

    Dopo aver creato la sottoscrizione è necessario confermarla tramite e-mail.
11. Per verificare la presenza di un messaggio di sottoscrizione, vai alla tua casella di posta elettronica e nel messaggio di sottoscrizione scegli Conferma sottoscrizione.

> **Note**
>
> Per verificare lo status dell'e-mail di conferma, vai alla console SNS e scegli Sottoscrizioni.

Per creare una EventBridge regola per acquisire i GuardDuty risultati e formattarli

1. Apri la EventBridge console all'indirizzo https://console.aws.amazon.com/events/.

2. Nel pannello di navigazione, scegli Regole.
3. Scegli Create rule (Crea regola).
4. Inserire un nome e una descrizione per la regola.

   Una regola non può avere lo stesso nome di un'altra regola nella stessa regione e sullo stesso router di eventi.
5. Per Event bus (Bus di eventi), scegli default.
6. Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).
7. Seleziona Successivo.
8. Per Event source (Origine eventi), seleziona AWS events (Eventi).
9. Per Modello di eventi, scegli Modulo di modello di eventi.
10. Per Origine evento, scegli Servizi AWS .
11. Per Servizio AWS , scegli GuardDuty.
12. Per Tipo di evento, scegli GuardDutyRicerca.
13. Seleziona Successivo.
14. Per Target types (Tipi di destinazione), scegli AWS service (Servizio).
15. Per Seleziona una destinazione, scegli Argomento SNS e per Argomento, scegli il nome dell'argomento SNS che hai creato in precedenza.
16. Nella sezione Impostazioni aggiuntive, per Configura input di destinazione, scegli Trasformatore di input.

    L'aggiunta di un trasformatore di input formatta i dati di ricerca JSON inviati GuardDuty in un messaggio leggibile dall'uomo.
17. Seleziona Configure input transformer (Configura trasformatore di input).
18. Nella sezione Trasformatore di input di destinazione, in Percorso di input, incolla il codice seguente:

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

```
}
```

19. Per formattare l'e-mail, in Template, incolla il codice seguente e assicurati di sostituire il testo in rosso con i valori appropriati alla tua regione:

```
"You have a severity severity GuardDuty finding type Finding_Type in
 the Region_Name Region."
"Finding Description:"
"Finding_Description."
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=region#/findings?search=id%3DFinding_ID"
```

20. Scegli Conferma.
21. Seleziona Successivo.
22. (Facoltativo) Inserire uno o più tag per la regola. Per ulteriori informazioni, consulta i EventBridge tag Amazon nella Amazon EventBridge User Guide.
23. Seleziona Successivo.
24. Rivedi i dettagli della regola e scegli Create rule (Crea regola).
25. (Facoltativo) Testa la tua nuova regola generando esiti di esempio con il processo descritto nella fase 2. Riceverai un'e-mail per ogni esito di esempio generato.

Passaggi successivi

Continuando a utilizzare GuardDuty, imparerai a comprendere i tipi di risultati pertinenti al tuo ambiente. Ogni volta che ricevi un nuovo esito, puoi trovare diverse informazioni, come i consigli su come correggerlo, selezionando Ulteriori informazioni dalla descrizione nel riquadro dei dettagli degli esiti o cercando il nome dell'esito su Tipi di esiti.

Le seguenti funzionalità ti aiuteranno a ottimizzare GuardDuty in modo che possa fornire i risultati più pertinenti per il tuo AWS ambiente:

- Per ordinare facilmente i risultati in base a criteri specifici, come l'ID dell'istanza, l'ID dell'account, il nome del bucket S3 e altro, puoi creare e salvare filtri all'interno. GuardDuty Per ulteriori informazioni, consulta Filtro dei risultati.
- Se ricevi esiti relativi al comportamento previsto nel tuo ambiente, puoi archiviarli automaticamente in base ai criteri definiti con le regole di eliminazione.

- Per evitare che i risultati vengano generati da un sottoinsieme di IP affidabili o per far sì che gli IP di GuardDuty monitoraggio non rientrino nel normale ambito di monitoraggio, puoi impostare elenchi di IP e minacce affidabili.

Concetti e terminologia

Quando inizi a usare Amazon GuardDuty, puoi trarre vantaggio dalla conoscenza dei suoi concetti chiave.

Account

Un account Amazon Web Services (AWS) standard che contiene AWS le tue risorse. Puoi accedere AWS con il tuo account e abilitare GuardDuty.

Puoi anche invitare altri account ad attivarsi GuardDuty e ad associarsi al tuo AWS account in GuardDuty. Se gli inviti vengono accettati, il tuo account viene designato come GuardDuty account amministratore e gli account aggiunti diventano i tuoi account membro. Puoi quindi visualizzare e gestire i GuardDuty risultati di tali account per loro conto.

Gli utenti dell'account amministratore possono configurare GuardDuty , visualizzare e gestire GuardDuty i risultati per il proprio account e per tutti gli account dei membri. Puoi avere fino a 10.000 account membri in GuardDuty.

Gli utenti degli account membro possono configurare GuardDuty , visualizzare e gestire GuardDuty i risultati nel proprio account (tramite la console di GuardDuty gestione o l' GuardDuty API). Gli utenti degli account membri non possono consultare o gestire i risultati negli account degli altri membri.

Un AWS account non può essere contemporaneamente un account GuardDuty amministratore e un account membro. Un account può accettare un solo invito AWS . L'accettazione di un invito è facoltativa.

Per ulteriori informazioni, consulta Gestione di più account in Amazon GuardDuty.

Rilevatore

Tutti i GuardDuty risultati sono associati a un rilevatore, che è un oggetto che rappresenta il GuardDuty servizio. Il rilevatore è un'entità regionale ed è necessario un rilevatore unico per ciascuna area in cui opera Regione AWS . GuardDuty Quando si abilita GuardDuty in una regione, viene generato un nuovo rilevatore con un DetectorID alfanumerico univoco di 32 caratteri. Il formato di un detectorId è `12abc34d567e8fa901bc2d34e56789f0`.

Per trovare le informazioni relative al `detectorId` tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

> **Note**
>
> Negli ambienti con più account, viene eseguito il roll up degli esiti di ogni account membro fino al rilevatore dell'account amministratore.

Alcune GuardDuty funzionalità vengono configurate tramite il rilevatore, ad esempio la configurazione della frequenza di notifica CloudWatch degli eventi e l'attivazione o la disabilitazione di fonti di dati opzionali da elaborare. GuardDuty

Origine dati

L'origine o la posizione di un set di dati. Per rilevare un'attività non autorizzata o imprevista nell'ambiente. AWS GuardDuty analizza ed elabora i dati provenienti da registri AWS CloudTrail eventi, eventi di AWS CloudTrail gestione, eventi di AWS CloudTrail dati per S3, log di flusso VPC, log DNS, log di audit EKS, monitoraggio delle attività di accesso RDS e volumi EBS. Per ulteriori informazioni, consulta Origini dati fondamentali.

Funzionalità

Un oggetto funzionale configurato per il piano di GuardDuty protezione consente di rilevare un'attività non autorizzata o imprevista nel proprio ambiente. AWS Ogni piano di GuardDuty protezione configura l'oggetto feature corrispondente per analizzare ed elaborare i dati. Alcuni oggetti funzionalità includono i log di audit EKS, il monitoraggio delle attività di accesso RDS e i volumi EBS. Per ulteriori informazioni, consulta Attivazione delle funzionalità in GuardDuty.

Risultato

Un potenziale problema di sicurezza rilevato da GuardDuty. Per ulteriori informazioni, consulta Comprendere i GuardDuty risultati di Amazon.

I risultati vengono visualizzati nella GuardDuty console e contengono una descrizione dettagliata del problema di sicurezza. Puoi anche recuperare i risultati generati chiamando le operazioni GetFindingse ListFindingsAPI.

Puoi anche visualizzare i GuardDuty risultati tramite Amazon CloudWatch Events. GuardDuty invia i risultati ad Amazon CloudWatch tramite il protocollo HTTPS. Per ulteriori informazioni, consulta Creazione di risposte personalizzate ai GuardDuty risultati con Amazon CloudWatch Events.

Opzioni di scansione

Quando la protezione GuardDuty da malware è abilitata, consente di specificare quali istanze Amazon EC2 e volumi Amazon Elastic Block Store (EBS) scansionare o ignorare. Grazie a questa funzionalità puoi aggiungere i tag esistenti associati alle istanze EC2 e al volume EBS a un elenco di tag di inclusione o di esclusione. Le risorse associate ai tag che aggiungi a un elenco di tag di inclusione vengono analizzate alla ricerca di malware, mentre quelle associate a un elenco di tag di esclusione non vengono scansionate. Per ulteriori informazioni, consulta Opzioni di scansione con tag definiti dall'utente.

Conservazione degli snapshot

Quando GuardDuty Malware Protection è abilitata, offre la possibilità di conservare le istantanee dei volumi EBS nel tuo account. AWS GuardDuty genera i volumi EBS di replica in base alle istantanee dei volumi EBS. Puoi conservare gli snapshot dei volumi EBS solo se la scansione della protezione da malware rileva il malware nei volumi EBS di replica, Se non viene rilevato alcun malware nei volumi EBS di replica, elimina GuardDuty automaticamente le istantanee dei volumi EBS, indipendentemente dall'impostazione di conservazione delle istantanee. Per ulteriori informazioni, consulta Conservazione degli snapshot.

Regole di soppressione

Le regole di soppressione automatica ti consentono di creare combinazioni di attributi molto specifiche per eliminare i risultati. Ad esempio, puoi definire una regola tramite il GuardDuty filtro per archiviare automaticamente `Recon:EC2/Portscan` solo le istanze in un VPC specifico, eseguendo un'AMI specifica o con un tag EC2 specifico. Questa regola comporterebbe l'archiviazione automatica dei risultati di scansione delle porte dalle istanze che soddisfano i criteri. Tuttavia, consente comunque di inviare avvisi se GuardDuty rileva che le istanze svolgono altre attività dannose, come il mining di criptovalute.

Le regole di soppressione definite nell' GuardDuty account amministratore si applicano agli account dei membri. GuardDuty GuardDuty gli account membri non possono modificare le regole di soppressione.

Con le regole di soppressione, genera GuardDuty comunque tutti i risultati. Le regole di soppressione consentono di sopprimere i risultati mantenendo nel contempo uno storico non modificabile di tutte le attività.

In genere, le regole di soppressione vengono utilizzate per nascondere i risultati che sono stati determinati come falsi positivi per l'ambiente e ridurre il rumore derivante da risultati di basso

valore, in modo da potersi concentrare sulle minacce più grandi. Per ulteriori informazioni, consulta Regole di eliminazione.

Elenco di indirizzi IP affidabili

Un elenco di indirizzi IP affidabili per comunicazioni altamente sicure con l' AWS ambiente in uso. GuardDuty non genera risultati basati su elenchi di IP affidabili. Per ulteriori informazioni, consulta Utilizzo di elenchi di indirizzi IP affidabili ed elenchi minacce.

Elenco di IP delle minacce

Un elenco degli indirizzi IP dannosi noti. Oltre a generare risultati a causa di un'attività potenzialmente sospetta, genera GuardDuty anche risultati basati su questi elenchi di minacce. Per ulteriori informazioni, consulta Utilizzo di elenchi di indirizzi IP affidabili ed elenchi minacce.

Attivazione delle funzionalità in GuardDuty

Quando abiliti Amazon GuardDuty per la prima volta o abiliti un tipo di protezione all'interno GuardDuty, GuardDuty avvia l'elaborazione del corrispondente Origini dati fondamentali all'interno del tuo AWS ambiente. GuardDuty utilizza queste fonti di dati per elaborare un flusso di eventi, come log di flusso VPC, log DNS e log di eventi e AWS CloudTrail di gestione. Successivamente analizza questi eventi per identificare potenziali minacce alla sicurezza e genera esiti nel tuo account.

Oltre alle fonti di dati di registro, GuardDuty può utilizzare dati aggiuntivi provenienti da altri AWS servizi AWS dell'ambiente per monitorare e analizzare potenziali minacce alla sicurezza.

Attivazioni delle funzionalità

Quando aggiungi GuardDuty protezioni aggiuntive, ad esempio S3 Protection, Runtime Monitoring o EKS Protection, puoi configurare la GuardDuty funzionalità corrispondente al tipo di protezione. Storicamente, GuardDuty le protezioni venivano `dataSources` richiamate nelle API. Tuttavia, dopo marzo 2023, i nuovi tipi di GuardDuty protezione sono ora configurati come `features` e non. `dataSources` GuardDuty supporta ancora la configurazione dei tipi di protezione lanciati prima di marzo 2023, come `dataSources` tramite l'API, ma i nuovi tipi di protezione sono disponibili solo come`features`.

Se gestisci i tipi di GuardDuty configurazione e protezione tramite la console, non sei direttamente interessato da questa modifica e non devi intraprendere alcuna azione. L'attivazione delle funzionalità influisce sul comportamento delle API richiamate per l'attivazione GuardDuty o sui tipi di protezione all'interno. GuardDuty Per ulteriori informazioni, consulta GuardDuty Modifiche all'API.

GuardDuty Modifiche alle API a marzo 2023

Le GuardDuty API configurano funzionalità di protezione che non appartengono all'elenco diOrigini dati fondamentali. Gli oggetti funzionalità contengono dettagli sulla funzionalità, come il nome e lo stato, e possono contenere configurazioni aggiuntive per alcune funzionalità. Questa migrazione riguarda le seguenti API in Amazon GuardDuty API Reference:

- CreateDetector
- GetDetector
- UpdateDetector

- GetMemberDetectors
- UpdateMemberDetectors
- DescribeOrganizationConfiguration
- UpdateOrganizationConfiguration
- GetRemainingFreeTrialDays
- GetUsageStatistics

Attivazione delle funzionalità rispetto alle origini dati

Storicamente, tutte le GuardDuty funzionalità venivano trasmesse attraverso un `dataSources` oggetto nell'API. A partire da marzo 2023, GuardDuty preferisce `features` l'oggetto anziché l'`dataSources`oggetto nell'API. Tutte le origini dati precedenti hanno funzionalità corrispondenti, ma le funzionalità più recenti potrebbero non avere origini dati corrispondenti.

L'elenco seguente mostra il confronto tra l'oggetto `dataSources` e l'oggetto `features` quando viene trasmesso tramite un'API:

- L'oggetto `dataSources` contiene oggetti per ogni tipo di protezione e il relativo stato. L'`features`oggetto è un elenco di funzionalità disponibili che corrispondono a ciascun tipo di protezione all'interno GuardDuty.

  A partire da marzo 2023, l'attivazione delle funzionalità sarà l'unico modo per configurare nuove GuardDuty funzionalità nel proprio AWS ambiente.
- Lo `dataSources` schema nella richiesta o nella risposta dell'API è lo stesso in tutti i paesi in Regione AWS cui GuardDuty è disponibile. Tuttavia, è possibile che non tutte le funzionalità siano disponibili in ogni regione. Pertanto, i nomi delle funzionalità disponibili possono variare in base alla regione.

Comprensione del funzionamento dell'attivazione delle funzionalità

Le GuardDuty API continueranno a restituire un `dataSources` oggetto, se applicabile, e restituiranno anche un `features` oggetto contenente le stesse informazioni in un formato diverso. GuardDuty le funzionalità lanciate prima di marzo 2023 saranno disponibili tramite `dataSources` object and `features` object. GuardDuty le funzionalità lanciate a partire da marzo 2023 saranno disponibili solo tramite l'`features`oggetto. Non puoi creare o aggiornare un rilevatore o descrivere il

tuo AWS Organizations utilizzando la notazione degli oggetti sia di `dataSources` che di `features` nella stessa richiesta API. Per abilitare i tipi di GuardDuty protezione, sarà necessario migrare le fonti di dati esistenti verso l'`features`oggetto utilizzando le stesse API che ora includono anche l'`features`oggetto.

> **Note**
>
> GuardDuty non aggiungerà una nuova fonte di dati dopo questa modifica.

GuardDuty ha reso obsoleto l'uso delle fonti di dati. Tuttavia, supporta ancora le Origini dati fondamentali. Le GuardDuty migliori pratiche consigliano di utilizzare l'attivazione delle funzionalità per tutti i tipi di protezione già abilitati per l'account. Le best practice richiedono anche l'utilizzo dell'attivazione delle funzionalità quando abiliti un nuovo tipo di protezione per il tuo account.

Incorporazione delle modifiche all'attivazione delle funzionalità

- Se gestisci GuardDuty le configurazioni tramite API, SDK o AWS CloudFormation template e desideri abilitare nuove potenziali GuardDuty funzionalità, dovrai modificare rispettivamente il codice e il modello. Per ulteriori informazioni, consulta le API aggiornate nell'Amazon GuardDuty API Reference.
- Per GuardDuty le funzionalità configurate prima di questo aggiornamento, puoi continuare a utilizzare le API, gli SDK o il modello. AWS CloudFormation Tuttavia, ti consigliamo di passare all'utilizzo dell'oggetto `feature`.

  Tutte le origini dati hanno un oggetto funzionalità equivalente. Per ulteriori informazioni, consulta Mappatura di `dataSources` su `features`.
- Attualmente, la `additionalConfiguration` nell'oggetto `features` è disponibile solo per determinati tipi di protezione.
  - Per questi tipi di protezione, se la funzionalità `AdditionalConfiguration` `status` è impostata su `ENABLED` ma la configurazione della funzionalità non `status` è impostata su`ENABLED`, non GuardDuty intraprenderà alcuna azione in questo caso.
  - Le seguenti API sono interessate:
    - UpdateDetector
    - UpdateMemberDetectors
    - UpdateOrganizationConfiguration

Mappatura di **`dataSources`** su **`features`**

La tabella seguente mostra la mappatura dei tipi di protezione, delle `dataSources` e delle `features`.

GuardDuty tipo di protezione	Nome della fonte di dati*	Nome della funzionalità
Log di flusso VPC	`flowLogs` (sola lettura; non possono essere modificati)	`FLOW_LOGS` (sola lettura; non possono essere modificati)
Log DNS	`dnsLogs` (sola lettura; non possono essere modificati)	`DNS_LOGS` (sola lettura; non possono essere modificati)
CloudTrail eventi	`cloudLogs` (sola lettura; non possono essere modificati)	`CLOUD_LOGS` (sola lettura; non possono essere modificati)
S3	`s3Logs`	`S3_DATA_EVENTS`
Monitoraggio dei log di audit EKS	`kubernetes.auditlogs`	`EKS_AUDIT_LOGS`
Protezione da malware	`malwareProtection.scanEc2InstanceWithFindings.ebsVolumes`	`EBS_MALWARE_PROTECTION`
Eventi di accesso RDS	GuardDuty fornisce solo il supporto per l'attivazione di funzionalità per questi tipi di protezione.	`RDS_LOGIN_EVENTS`

GuardDuty tipo di protezione	Nome della fonte di dati*	Nome della funzionalità
Monitoraggio del runtime EKS		`EKS_RUNTIME_MONITORING`
Monitoraggio del runtime		`RUNTIME_MONITORING`
GuardDuty agente di sicurezza per cluster Amazon EKS		`EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT` `RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`
GuardDuty agente di sicurezza per cluster Amazon ECS		`RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT`

GuardDuty tipo di protezione	Nome della fonte di dati*	Nome della funzionalità
Protezione Lambda		`LAMBDA_NETWORK_LOGS`

*GetUsageStatistics utilizza i propri nomi di `dataSource`. Per ulteriori informazioni, consultare Stima dei costi GuardDuty o GetUsageStatistics.

Origini dati fondamentali

GuardDuty utilizza le fonti di dati fondamentali per rilevare le comunicazioni con domini e indirizzi IP dannosi noti e identificare comportamenti anomali. Durante il transito da queste fonti a GuardDuty, tutti i dati di registro vengono crittografati. GuardDutyestrae vari campi da queste fonti di log per la profilazione e il rilevamento delle anomalie, quindi elimina questi registri.

Le sezioni seguenti descrivono come GuardDuty utilizza ciascuna fonte di dati supportata. Quando lo GuardDuty abiliti Account AWS, inizia GuardDuty automaticamente a monitorare queste fonti di registro.

Argomenti

- AWS CloudTrail registri degli eventi
- AWS CloudTrail eventi gestionali
- Log di flusso VPC
- Log DNS

AWS CloudTrail registri degli eventi

AWS CloudTrail fornisce una cronologia delle chiamate AWS API per il tuo account, incluse le chiamate API effettuate utilizzando gli AWS SDK AWS Management Console, gli strumenti da riga di comando e determinati AWS servizi. CloudTrail ti aiuta anche a identificare quali utenti e account hanno richiamato le AWS API per i servizi che supportano CloudTrail, l'indirizzo IP di origine da cui sono state richiamate le chiamate e l'ora in cui sono state richiamate le chiamate. Per ulteriori informazioni, consulta Che cos'è AWS CloudTrail? nella Guida per l'utente di AWS CloudTrail .

GuardDuty monitora anche gli eventi di gestione. CloudTrail Quando lo abiliti GuardDuty, inizia a consumare gli eventi di CloudTrail gestione direttamente CloudTrail attraverso un flusso di eventi indipendente e duplicato e analizza i CloudTrail registri degli eventi. Non sono previsti costi aggiuntivi per l' GuardDuty accesso agli eventi registrati in. CloudTrail

GuardDuty non gestisce i tuoi CloudTrail eventi né influisce sulle CloudTrail configurazioni esistenti. Allo stesso modo, le CloudTrail configurazioni non influiscono sul modo in cui GuardDuty utilizza ed elabora i registri degli eventi. Per gestire l'accesso e la conservazione dei tuoi CloudTrail eventi, utilizza la console di CloudTrail servizio o l'API. Per ulteriori informazioni, consulta Visualizzazione degli eventi con cronologia degli CloudTrail eventi nella Guida AWS CloudTrail per l'utente.

Come GuardDuty gestisce gli eventi AWS CloudTrail globali

Per la maggior parte AWS dei servizi, CloudTrail gli eventi vengono registrati nel Regione AWS luogo in cui vengono creati. Per i servizi globali come AWS Identity and Access Management (IAM), AWS Security Token Service (AWS STS), Amazon Simple Storage Service (Amazon S3), CloudFront Amazon e Amazon Route 53 (Route 53), gli eventi vengono generati solo nella regione in cui si verificano, ma hanno un'importanza globale.

Quando GuardDuty utilizza eventi di servizio CloudTrail globali con valori di sicurezza come configurazioni di rete o autorizzazioni utente, replica tali eventi e li elabora in ogni regione in cui sono stati abilitati. GuardDuty Questo comportamento aiuta a GuardDuty mantenere i profili utente e di ruolo in ogni regione, il che è fondamentale per rilevare eventi anomali.

Ti consigliamo vivamente di abilitare GuardDuty tutto ciò che è abilitato per Regioni AWS il tuo. Account AWS Ciò aiuta a GuardDuty generare informazioni su attività non autorizzate o insolite anche in quelle regioni che potresti non utilizzare attivamente.

AWS CloudTrail eventi gestionali

Gli eventi di gestione sono noti anche come eventi del piano di controllo (control-plane). Questi eventi forniscono informazioni dettagliate sulle operazioni di gestione eseguite sulle risorse del tuo AWS account.

Di seguito sono riportati alcuni esempi di eventi CloudTrail gestionali GuardDuty monitorati:

- Configurazione della sicurezza (operazioni API `AttachRolePolicy` di IAM)
- Configurazione di regole per l'instradamento dei dati (operazioni API `CreateSubnet` di Amazon EC2)
- Configurazione della registrazione (operazioni AWS CloudTrail `CreateTrail` API)

Log di flusso VPC

La funzionalità VPC Flow Logs di Amazon VPC acquisisce informazioni sul traffico IP in entrata e in uscita dalle interfacce di rete collegate alle istanze Amazon Elastic Compute Cloud (Amazon EC2) all'interno del tuo ambiente. AWS

Quando lo abiliti GuardDuty, inizia immediatamente ad analizzare i log di flusso VPC dalle istanze Amazon EC2 all'interno del tuo account. Utilizza gli eventi di tali log direttamente dalla funzionalità

Log di flusso VPC tramite un flusso indipendente e ridondante di log di flusso. Questo processo non altera alcuna configurazione di log di flusso esistente.

GuardDuty Protezione Lambda

Lambda Protection è un miglioramento opzionale di Amazon. GuardDuty Attualmente, il monitoraggio delle attività di rete Lambda include i log di flusso di Amazon VPC di tutte le funzioni Lambda del tuo account, anche quelli che non utilizzano reti VPC. Per proteggere la tua funzione Lambda da potenziali minacce alla sicurezza, dovrai configurare Lambda Protection nel tuo account. GuardDuty Per ulteriori informazioni, consulta GuardDuty Protezione Lambda.

GuardDuty Monitoraggio del runtime

Quando gestisci l'agente di sicurezza (manualmente o tramite GuardDuty) in EKS Runtime Monitoring o Runtime Monitoring for EC2 e GuardDuty viene attualmente distribuito su un'istanza Amazon EC2 e riceve i dati Tipi di eventi di runtime raccolti da questa istanza, non GuardDuty ti verrà addebitato alcun costo per Account AWS l'analisi dei log di flusso VPC da questa istanza Amazon EC2. Questo aiuta a GuardDuty evitare il doppio dei costi di utilizzo dell'account.

GuardDuty non gestisce i log di flusso né li rende accessibili nel tuo account. Per gestire l'accesso dei log di flusso e la loro conservazione, devi configurare la funzionalità Log di flusso VPC.

Log DNS

Se utilizzi resolver AWS DNS per le tue istanze Amazon EC2 (l'impostazione predefinita), GuardDuty puoi accedere ed elaborare i log DNS di richiesta e risposta tramite i resolver DNS interni. AWS Se utilizzi un altro resolver DNS, come OpenDNS o GoogleDNS, o se configuri i tuoi resolver DNS, non puoi accedere ed elaborare i dati da questa fonte di dati. GuardDuty

Quando lo abiliti GuardDuty, inizia immediatamente ad analizzare i log DNS da un flusso di dati indipendente. Questo flusso di dati è separato dai dati forniti tramite la funzionalità di Registrazione delle query del Route 53 Resolver. La configurazione di questa funzionalità non influisce sull'analisi. GuardDuty

> **Note**
>
> GuardDuty non supporta il monitoraggio dei log DNS per le istanze Amazon EC2 avviate AWS Outposts su perché Amazon Route 53 Resolver la funzionalità di registrazione delle query non è disponibile in quell'ambiente.

Protezione EKS in Amazon GuardDuty

Il monitoraggio dei log di audit EKS è utile per rilevare attività potenzialmente sospette nei cluster EKS all'interno di Amazon Elastic Kubernetes Service (Amazon EKS). Il monitoraggio dei log di audit EKS utilizza i log di audit di Kubernetes per acquisire le attività cronologiche degli utenti, delle applicazioni che utilizzano l'API Kubernetes e il piano di controllo (control-plane). Per ulteriori informazioni, consulta Log di audit di Kubernetes.

> **Note**
>
> EKS Runtime Monitoring è gestito come parte di Runtime Monitoring. Per ulteriori informazioni, consulta GuardDuty Monitoraggio del runtime.

Funzionalità di Protezione EKS

Log di audit di Kubernetes

I log di audit di Kubernetes acquisiscono le operazioni sequenziali all'interno del cluster Amazon EKS, incluse le attività degli utenti, le applicazioni che utilizzano l'API Kubernetes e il piano di controllo (control-plane). La registrazione di audit è un componente di tutti i cluster Kubernetes.

Per ulteriori informazioni, consultare Auditing nella documentazione Kubernetes.

Amazon EKS consente di importare i log di audit di Kubernetes come Amazon CloudWatch Logs tramite la funzionalità di registrazione del piano di controllo EKS. GuardDuty non gestisce la registrazione del piano di controllo di Amazon EKS né rende accessibili i log di audit di Kubernetes nel tuo account se non li hai abilitati per Amazon EKS. Per gestire l'accesso e la conservazione dei log di audit di Kubernetes, devi configurare la funzionalità di registrazione del piano di controllo (control-plane) Amazon EKS. Per ulteriori informazioni, consulta Abilitazione e disabilitazione dei log del piano di controllo nella Guida per l'utente di Amazon EKS.

Per informazioni sulla configurazione del monitoraggio dei log di audit EKS, consulta Monitoraggio dei log di audit EKS.

Monitoraggio dei log di audit EKS

Il monitoraggio dei log di audit EKS è utile per rilevare attività potenzialmente sospette nei cluster EKS all'interno di Amazon Elastic Kubernetes Service. Quando abiliti EKS Audit Log Monitoring, inizia GuardDuty immediatamente Log di audit di Kubernetes a monitorare i cluster Amazon EKS e ad analizzarli per attività potenzialmente dannose e sospette. Utilizza gli eventi dei log di controllo Kubernetes direttamente dalla funzionalità di registrazione del piano di controllo di Amazon EKS attraverso un flusso indipendente e duplicato di log di audit. Questo processo non richiede alcuna configurazione aggiuntiva né influisce sulle configurazioni di registrazione del piano di controllo (control-plane) Amazon EKS esistenti che potresti avere.

Quando disabiliti EKS Audit Log Monitoring, interrompe GuardDuty immediatamente il monitoraggio e l'analisi dei log di audit Kubernetes per le tue risorse Amazon EKS.

EKS Audit Log Monitoring potrebbe non essere disponibile ovunque sia disponibile. Regioni AWS GuardDuty Per ulteriori informazioni, consulta Disponibilità di funzionalità specifiche per ogni regione.

In che modo il periodo di prova gratuito di 30 giorni influisce sugli account GuardDuty

- Quando si attiva GuardDuty per la prima volta, EKS Audit Log Monitoring all'interno di EKS Protection è già incluso nel periodo di prova gratuito di 30 giorni.
- GuardDuty Gli account esistenti possono abilitare EKS Audit Log Monitoring per la prima volta con un periodo di prova gratuito di 30 giorni.

Configurazione del monitoraggio dei log di audit EKS per un account autonomo

Scegli il metodo di accesso che preferisci per abilitare o disabilitare il monitoraggio dei log di audit EKS per un account autonomo.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Protezione EKS.
3. Nella scheda Configurazione, puoi visualizzare lo stato di configurazione attuale del monitoraggio dei log di audit EKS. Nella sezione Monitoraggio dei log di audit EKS, scegli Abilita per abilitare o Disabilita per disabilitare la funzionalità di monitoraggio dei log di audit EKS.

4. Selezionare Salva.

API/CLI

- Esegui l'operazione updateDetectorAPI utilizzando l'ID del rilevatore regionale dell'account GuardDuty amministratore delegato e passando il nome dell'`features`oggetto come `EKS_AUDIT_LOGS` e lo status come `ENABLED` o. `DISABLED`

  In alternativa, è anche possibile abilitare o disabilitare EKS Audit Log Monitoring eseguendo il comando a AWS CLI . Il seguente codice di esempio abilita GuardDuty EKS Audit Log Monitoring. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

  Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

Configurazione del monitoraggio dei log di audit EKS in ambienti con più account

In un ambiente con più account, solo l'account GuardDuty amministratore delegato ha la possibilità di abilitare o disabilitare la funzionalità EKS Audit Log Monitoring per gli account membri della propria organizzazione. GuardDuty Gli account membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce i propri account membro utilizzando AWS Organizations. Questo account GuardDuty amministratore delegato può scegliere di abilitare automaticamente EKS Audit Log Monitoring per tutti i nuovi account quando entrano a far parte dell'organizzazione. Per ulteriori informazioni sugli ambienti con più account, consulta Gestione di più account in Amazon. GuardDuty

Configurazione di EKS Audit Log Monitoring per un account amministratore delegato GuardDuty

Scegliete il metodo di accesso preferito per configurare EKS Audit Log Monitoring per l'account amministratore delegato. GuardDuty

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

Assicurati di utilizzare le credenziali dell'account di gestione.

2. Nel riquadro di navigazione, scegli Protezione EKS.
3. Nella scheda Configurazione, puoi visualizzare lo stato di configurazione attuale del monitoraggio dei log di audit EKS nella sezione corrispondente. Per aggiornare la configurazione per l'account GuardDuty amministratore delegato, scegliete Modifica nel riquadro EKS Audit Log Monitoring.
4. Esegui una di queste operazioni:

   Utilizzando Abilita per tutti gli account

   - Scegli Abilita per tutti gli account. Ciò abiliterà il piano di protezione per tutti gli GuardDuty account attivi nell' AWS organizzazione, inclusi i nuovi account che entrano a far parte dell'organizzazione.
   - Selezionare Salva.

   Utilizzando Configura gli account manualmente

   - Per abilitare il piano di protezione solo per l'account GuardDuty amministratore delegato, scegli Configura gli account manualmente.
   - Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).
   - Selezionare Salva.

API/CLI

Esegui l'operazione API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il `name` dell'oggetto `features` su `EKS_AUDIT_LOGS` e lo `status` su `ENABLED` o `DISABLED`.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

È possibile abilitare o disabilitare EKS Audit Log Monitoring eseguendo il seguente AWS CLI comando. Assicurati di utilizzare l'ID *`rilevatore`* valido dell'account GuardDuty amministratore delegato.

> **Note**
>
> Il codice di esempio seguente abilita il monitoraggio dei log di audit EKS. *Assicurati di sostituire 12abc34d567e8fa901bc2d34e56789f0 con quello dell'account amministratore delegato e 5555 con quello dell'account amministratore delegato. detector-id GuardDuty* Account AWS GuardDuty

Per `detectorId` trovare le informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 555555555555 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

Per disabilitare il monitoraggio dei log di audit EKS, sostituisci `ENABLED` con `DISABLED`.

Abilitare automaticamente il monitoraggio dei log di audit EKS per tutti gli account membri

Scegli il metodo di accesso che preferisci per abilitare il monitoraggio dei log di audit EKS per account membri esistenti dell'organizzazione.

Console

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una di queste operazioni:

   Utilizzando la pagina Protezione EKS

   1. Nel riquadro di navigazione, scegli Protezione EKS.
   2. Nella scheda Configurazione, puoi visualizzare lo stato attuale del monitoraggio dei log di audit EKS per gli account membri attivi dell'organizzazione.

      Per aggiornare la configurazione del monitoraggio dei log di audit EKS, scegli Modifica.

3. Scegli Abilita per tutti gli account. Questa operazione abilita automaticamente il monitoraggio dei log di audit EKS per gli account dell'organizzazione esistenti e per quelli nuovi.
4. Selezionare Salva.

> **Note**
>
> L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Utilizzando la pagina Account

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
3. Nella finestra Gestisci le preferenze di abilitazione automatica, scegli Abilita per tutti gli account in Monitoraggio dei log di audit EKS.
4. Selezionare Salva.

Se non puoi utilizzare l'opzione Abilita per tutti gli account e desideri personalizzare la configurazione del monitoraggio dei log di audit EKS per account specifici dell'organizzazione, consulta Abilitare o disabilitare in modo selettivo il monitoraggio dei log di audit EKS per gli account membri.

API/CLI

- Per abilitare o disabilitare in modo selettivo il monitoraggio dei log di audit EKS per i tuoi account membri, esegui l'operazione API updateMemberDetectors utilizzando il tuo *`ID rilevatore`*.
- L'esempio seguente mostra come abilitare il monitoraggio dei log di audit EKS per un singolo account membro. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

  Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

> **Note**
>
> Puoi anche trasmettere un elenco di ID account separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare il monitoraggio dei log di audit EKS per tutti gli account membri attivi esistenti

Scegli il metodo di accesso che preferisci per abilitare il monitoraggio dei log di audit EKS per tutti gli account membri attivi esistenti dell'organizzazione.

Console

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.
2. Nel riquadro di navigazione, scegli Protezione EKS.
3. Nella pagina EKS Protection, è possibile visualizzare lo stato corrente della configurazione della scansione GuardDutyantimalware avviata. Nella sezione Account membri attivi, scegli Operazioni.
4. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
5. Selezionare Salva.

API/CLI

- Per abilitare o disabilitare in modo selettivo il monitoraggio dei log di audit EKS per i tuoi account membri, esegui l'operazione API updateMemberDetectors utilizzando il tuo *ID rilevatore*.

- L'esempio seguente mostra come abilitare il monitoraggio dei log di audit EKS per un singolo account membro. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

  Per trovare la `detectorId` regione relativa al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

  > **Note**
  >
  > Puoi anche trasmettere un elenco di ID account separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare automaticamente il monitoraggio dei log di audit EKS per i nuovi account membri

Gli account membro appena aggiunti devono essere abilitati GuardDuty prima di selezionare la configurazione della scansione GuardDuty antimalware avviata. Gli account membri gestiti su invito possono configurare manualmente la scansione antimalware GuardDuty avviata per i propri account. Per ulteriori informazioni, consulta Step 3 - Accept an invitation.

Scegli il metodo di accesso che preferisci per abilitare il monitoraggio dei log di audit EKS per i nuovi account che entrano a far parte dell'organizzazione.

Console

L'account GuardDuty amministratore delegato può abilitare EKS Audit Log Monitoring per i nuovi account membro di un'organizzazione, utilizzando la pagina EKS Audit Log Monitoring o Accounts.

Per abilitare automaticamente il monitoraggio dei log di audit EKS per i nuovi account membri

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una di queste operazioni:
   - Utilizzando la pagina Protezione EKS:
     1. Nel riquadro di navigazione, scegli Protezione EKS.
     2. Nella pagina Protezione EKS, scegli Modifica nel monitoraggio dei log di audit EKS.
     3. Scegli Configura gli account manualmente.
     4. Seleziona Abilita automaticamente per i nuovi account membri. Questa fase garantisce l'abilitazione automatica del monitoraggio dei log di audit EKS per ogni nuovo account che entra a far parte dell'organizzazione. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa configurazione.
     5. Selezionare Salva.
   - Utilizzando la pagina Account:
     1. Dal riquadro di navigazione, selezionare Accounts (Account).
     2. Nella pagina Account, scegli le preferenze di Abilitazione automatica.
     3. Nella finestra Gestisci le preferenze di abilitazione automatica, seleziona Abilita per nuovi account in Monitoraggio dei log di audit EKS.
     4. Selezionare Salva.

API/CLI

- Per abilitare o disabilitare in modo selettivo il monitoraggio dei log di audit EKS per i tuoi nuovi account, esegui l'operazione API UpdateOrganizationConfiguration utilizzando il tuo *ID rilevatore*.
- L'esempio seguente mostra come abilitare il monitoraggio dei log di audit EKS per i nuovi membri che entrano a far parte dell'organizzazione. Puoi anche trasmettere un elenco di ID account separati da uno spazio.

  Per trovare l'`detectorId`account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

Abilitare o disabilitare in modo selettivo il monitoraggio dei log di audit EKS per gli account membri

Scegli il metodo di accesso che preferisci per abilitare o disabilitare il monitoraggio dei log di audit EKS per account membri selettivi dell'organizzazione.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.
2. Dal riquadro di navigazione, selezionare Accounts (Account).

   Nella pagina Account, consulta la colonna Monitoraggio dei log di audit EKS per visualizzare lo stato del tuo account membro.
3. Abilitare o disabilitare il monitoraggio dei log di audit EKS

   Seleziona un account da configurare per il monitoraggio dei log di audit EKS. Puoi selezionare più account alla volta. Nel menu a discesa Modifica piani di protezione, scegli Monitoraggio dei log di audit EKS, quindi scegli l'opzione appropriata.

API/CLI

Per abilitare o disabilitare in modo selettivo il monitoraggio dei log di audit EKS per i tuoi account membri, richiama l'operazione API updateMemberDetectors utilizzando il tuo *`ID rilevatore`*.

L'esempio seguente mostra come abilitare il monitoraggio dei log di audit EKS per un singolo account membro. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`. Puoi anche trasmettere un elenco di ID account separati da uno spazio.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

Protezione Lambda in Amazon GuardDuty

La Protezione Lambda è utile per identificare potenziali minacce alla sicurezza quando una funzione AWS Lambda viene richiamata nel tuo ambiente AWS . Quando abiliti Lambda Protection, GuardDuty inizia a monitorare i registri delle attività di rete Lambda, a partire da Log di flusso VPC tutte le funzioni Lambda per account, inclusi i registri che non utilizzano la rete VPC, e vengono generati quando viene richiamata la funzione Lambda. Se GuardDuty identifica un traffico di rete sospetto che è indicativo della presenza di un pezzo di codice potenzialmente dannoso nella funzione Lambda, GuardDuty genererà un risultato.

> **Note**
>
> Il monitoraggio delle attività di rete Lambda non include i log per le funzioni Lambda @Edge.

Puoi configurare Lambda Protection per qualsiasi account o disponibile Regioni AWS, in qualsiasi momento. Per impostazione predefinita, un GuardDuty account esistente può abilitare Lambda Protection con un periodo di prova di 30 giorni. Per un nuovo GuardDuty account, Lambda Protection è già abilitata e inclusa nel periodo di prova di 30 giorni. Per informazioni sulle statistiche di utilizzo, consulta Stima del costo.

GuardDuty monitora i registri delle attività di rete generati richiamando le funzioni Lambda. Attualmente, il monitoraggio delle attività di rete Lambda include i log di flusso Amazon VPC di tutte le funzioni Lambda del tuo account, tra cui i log che non utilizzano reti VPC e che sono soggetti a modifiche, inclusa l'espansione ad altre attività di rete come i dati relativi a query DNS generati richiamando le funzioni Lambda. L'espansione ad altre forme di monitoraggio delle attività di rete aumenterà il volume di dati che GuardDuty verranno elaborati per Lambda Protection. il che avrà un impatto diretto sul costo di utilizzo di questa protezione. Ogni volta che GuardDuty inizia a monitorare un registro delle attività di rete aggiuntivo, fornirà un avviso agli account che hanno attivato Lambda Protection, almeno 30 giorni prima del rilascio.

Funzionalità della Protezione Lambda

Monitoraggio delle attività di rete Lambda

Quando abiliti Lambda Protection, GuardDuty monitora i registri delle attività di rete Lambda generati quando viene richiamata una funzione Lambda associata al tuo account. Ciò consente di rilevare

potenziali minacce alla sicurezza della funzione Lambda. GuardDuty monitora i log di flusso VPC di tutte le funzioni Lambda, comprese quelle che non utilizzano reti VPC. Per le funzioni Lambda configurate per utilizzare la rete VPC, non è necessario abilitare i log di flusso VPC per le interfacce di rete elastiche (ENI) create da Lambda for. GuardDuty GuardDuty addebita solo la quantità di dati dei registri delle attività di rete Lambda elaborati (in GB) per generare un risultato. GuardDuty ottimizza i costi applicando filtri intelligenti e analizzando un sottoinsieme di registri delle attività di rete Lambda rilevanti per il rilevamento delle minacce. Per informazioni sui prezzi, consulta la pagina GuardDuty dei prezzi di Amazon.

GuardDuty non gestisce i registri delle attività della rete Lambda (inclusi i log di flusso VPC e non VPC) né li rende accessibili nel tuo account.

Configurazione della Protezione Lambda

Configurazione della Protezione Lambda per un account autonomo

Per gli account associati a AWS Organizations, puoi automatizzare questo processo tramite le istruzioni della GuardDuty console o dell'API, come descritto nella sezione successiva.

Scegli il metodo di accesso che preferisci per abilitare o disabilitare la Protezione Lambda per un account autonomo.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, in Impostazioni, scegli Protezione Lambda.
3. La pagina della Protezione Lambda mostra lo stato attuale del tuo account. Puoi abilitare o disabilitare la funzionalità in qualsiasi momento selezionando Abilita o Disabilita.
4. Selezionare Salva.

API/CLI

Esegui l'operazione API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il `name` dell'oggetto `features` su `LAMBDA_NETWORK_LOGS` e lo `status` su `ENABLED` o `DISABLED`.

Puoi anche abilitare o disabilitare il monitoraggio dell'attività di rete Lambda eseguendo il comando seguente AWS CLI . Assicurati di utilizzare il tuo *`ID rilevatore`* valido.

> **Note**
>
> Il codice di esempio seguente abilita il monitoraggio delle attività di rete Lambda. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

Configurazione della Protezione Lambda in ambienti multi-account

In un ambiente con più account, solo l'account GuardDuty amministratore delegato ha la possibilità di abilitare o disabilitare Lambda Protection per gli account dei membri della propria organizzazione. GuardDuty Gli account membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce gli account dei membri utilizzando AWS Organizations. L'account GuardDuty amministratore delegato può scegliere di abilitare automaticamente il monitoraggio dell'attività di rete Lambda per tutti i nuovi account quando entrano a far parte dell'organizzazione. Per ulteriori informazioni sugli ambienti con più account, consulta Gestione di più account in Amazon GuardDuty.

Configurazione di Lambda Protection per GuardDuty l'account amministratore delegato

Scegli il tuo metodo di accesso preferito per abilitare o disabilitare il monitoraggio dell'attività di rete Lambda per l'account amministratore delegato GuardDuty .

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali dell'account di gestione.
2. Nel riquadro di navigazione, in Impostazioni, scegli Protezione Lambda.
3. Nella pagina Protezione Lambda, scegli Modifica.
4. Esegui una di queste operazioni:

Utilizzando Abilita per tutti gli account

- Scegli Abilita per tutti gli account. Ciò abiliterà il piano di protezione per tutti gli GuardDuty account attivi AWS dell'organizzazione, inclusi i nuovi account che entrano a far parte dell'organizzazione.
- Selezionare Salva.

Utilizzando Configura gli account manualmente

- Per abilitare il piano di protezione solo per l'account GuardDuty amministratore delegato, scegli Configura gli account manualmente.
- Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).
- Selezionare Salva.

API/CLI

Esegui l'operazione API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il `name` dell'oggetto `features` su `LAMBDA_NETWORK_LOGS` e lo `status` su `ENABLED` o `DISABLED`.

È possibile abilitare o disabilitare il monitoraggio dell'attività di rete Lambda eseguendo il comando seguente AWS CLI . Assicurati di utilizzare l'ID *`rilevatore`* valido dell'account GuardDuty amministratore delegato.

> **Note**
>
> Il codice di esempio seguente abilita il monitoraggio delle attività di rete Lambda. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 555555555555 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status":
 "ENABLED"}]'
```

Abilitare automaticamente il monitoraggio delle attività di rete Lambda per tutti gli account membri

Scegli il metodo di accesso che preferisci per abilitare la funzionalità di monitoraggio delle attività di rete Lambda per tutti gli account membri, inclusi gli account membri esistenti e i nuovi account che entrano a far parte dell'organizzazione.

Console

1. Accedi a AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una di queste operazioni:

   Utilizzando la pagina Protezione Lambda

   1. Nel riquadro di navigazione, scegli Protezione Lambda.
   2. Scegli Abilita per tutti gli account. Questa operazione abilita automaticamente il monitoraggio delle attività di rete Lambda per gli account dell'organizzazione esistenti e per quelli nuovi.
   3. Selezionare Salva.

   > **Note**
   >
   > L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

   Utilizzando la pagina Account

   1. Dal riquadro di navigazione, selezionare Accounts (Account).
   2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
   3. Nella finestra Gestisci le preferenze di abilitazione automatica, scegli Abilita per tutti gli account in Monitoraggio delle attività di rete Lambda.

> **Note**
>
> Per impostazione predefinita, questa azione attiva automaticamente l'opzione Attivazione automatica GuardDuty per nuovi account membro.

4. Selezionare Salva.

Se non puoi utilizzare l'opzione Abilita per tutti gli account, consulta Abilitare o disabilitare in modo selettivo il monitoraggio delle attività di rete Lambda per gli account membri.

API/CLI

- Per abilitare o disabilitare in modo selettivo il monitoraggio delle attività di rete Lambda per i tuoi account membri, richiama l'operazione API updateMemberDetectors utilizzando il tuo *ID rilevatore*.
- L'esempio seguente mostra come abilitare il monitoraggio delle attività di rete Lambda per un singolo account membro. Per disabilitare un account membro, sostituisci `ENABLED` con `DISABLED`.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

  Puoi anche trasmettere un elenco di ID account separati da uno spazio.
- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare il monitoraggio delle attività di rete Lambda per tutti gli account membri attivi esistenti

Scegli il metodo di accesso che preferisci per abilitare il monitoraggio delle attività di rete Lambda per tutti gli account membri attivi esistenti dell'organizzazione.

Console

Per configurare il monitoraggio delle attività di rete Lambda per tutti gli account membri attivi esistenti

1. Accedi a AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.
2. Nel riquadro di navigazione, scegli Protezione Lambda.
3. Nella pagina Protezione Lambda, puoi visualizzare lo stato attuale della configurazione. Nella sezione Account membri attivi, scegli Operazioni.
4. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
5. Scegli Conferma.

API/CLI

- Per abilitare o disabilitare in modo selettivo il monitoraggio delle attività di rete Lambda per i tuoi account membri, richiama l'operazione API updateMemberDetectors utilizzando il tuo *ID rilevatore*.
- L'esempio seguente mostra come abilitare il monitoraggio delle attività di rete Lambda per un singolo account membro. Per disabilitare un account membro, sostituisci `ENABLED` con `DISABLED`.

  Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

  Puoi anche trasmettere un elenco di ID account separati da uno spazio.
- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare automaticamente il monitoraggio delle attività di rete Lambda per i nuovi account membri

Scegli il metodo di accesso che preferisci per abilitare il monitoraggio delle attività di rete Lambda per i nuovi account che entrano a far parte dell'organizzazione.

Console

L'account GuardDuty amministratore delegato può abilitare il monitoraggio dell'attività di rete Lambda per i nuovi account membro di un'organizzazione, utilizzando la pagina Lambda Protection o Account.

Per abilitare automaticamente il monitoraggio delle attività di rete Lambda per i nuovi account membri

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.
2. Esegui una di queste operazioni:
   - Utilizzando la pagina Protezione Lambda:
     1. Nel riquadro di navigazione, scegli Protezione Lambda.
     2. Nella pagina Protezione Lambda, scegli Modifica.
     3. Scegli Configura gli account manualmente.
     4. Seleziona Abilita automaticamente per i nuovi account membri. Questa fase garantisce l'abilitazione automatica della Protezione Lambda per ogni nuovo account che entra a far parte dell'organizzazione. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa configurazione.
     5. Selezionare Salva.
   - Utilizzando la pagina Account:
     1. Dal riquadro di navigazione, selezionare Accounts (Account).
     2. Nella pagina Account, scegli le preferenze di Abilitazione automatica.
     3. Nella finestra Gestisci le preferenze di abilitazione automatica, seleziona Abilita per nuovi account in Monitoraggio delle attività di rete Lambda.
     4. Selezionare Salva.

API/CLI

- Per abilitare o disabilitare il monitoraggio delle attività di rete Lambda per i nuovi account membri, richiama l'operazione API UpdateOrganizationConfiguration utilizzando il tuo *ID rilevatore*.
- L'esempio seguente mostra come abilitare il monitoraggio delle attività di rete Lambda per un singolo account membro. Per disabilitarlo, consulta Abilitare o disabilitare in modo selettivo il monitoraggio delle attività di rete Lambda per gli account membri. Se non desideri abilitarlo per tutti i nuovi account che entrano a far parte dell'organizzazione, imposta `AutoEnable` su `NONE`.

  Per trovare l'`detectorId`account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

  Puoi anche trasmettere un elenco di ID account separati da uno spazio.
- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare o disabilitare in modo selettivo il monitoraggio delle attività di rete Lambda per gli account membri

Scegli il metodo di accesso che preferisci per abilitare o disabilitare in modo selettivo il monitoraggio delle attività di rete Lambda per gli account membri.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.
2. Nel riquadro di navigazione, in Settings (Impostazioni), scegliere Accounts (Account).

   Nella pagina Account, consulta la colonna Monitoraggio delle attività di rete Lambda, che indica se il monitoraggio delle attività di rete Lambda è abilitato o meno.

3. Scegli l'account per il quale desideri configurare la Protezione Lambda. Puoi scegliere più account alla volta.
4. Dal menu a discesa Modifica piani di protezione, scegli Monitoraggio delle attività di rete Lambda, quindi scegli l'operazione appropriata.

API/CLI

Richiama l'API updateMemberDetectors utilizzando il tuo *`ID rilevatore`*.

L'esempio seguente mostra come abilitare il monitoraggio delle attività di rete Lambda per un singolo account membro. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

Puoi anche trasmettere un elenco di ID account separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Protezione da malware in Amazon GuardDuty

La protezione da malware è utile per rilevare la potenziale presenza di malware eseguendo la scansione dei Volumi Amazon Elastic Block Store (Amazon EBS) collegati alle istanze Amazon Elastic Compute Cloud (Amazon EC2) e ai carichi di lavoro di un container. Questa protezione offre diverse opzioni per cui puoi decidere se includere o escludere istanze Amazon EC2 e carichi di lavoro di un container specifici al momento della scansione, Offre inoltre la possibilità di conservare le istantanee dei volumi Amazon EBS collegati alle istanze Amazon EC2 o ai carichi di lavoro dei container nei tuoi account. GuardDuty Gli snapshot vengono conservati solo in caso di rilevamento di malware e di generazione di esiti della protezione da malware.

Malware Protection offre due tipi di scansioni per rilevare attività potenzialmente dannose nelle istanze Amazon EC2 e nei carichi di lavoro dei container GuardDuty: la scansione antimalware avviata e la scansione antimalware su richiesta. La tabella seguente mostra il confronto tra i due tipi di scansione.

Factor	GuardDuty-scansione antimalware avviata	Scansione antimalware on demand
Come viene richiamata la scansione	Dopo aver GuardDuty abilitato la scansione antimalwa re avviata, ogni volta che GuardDuty genera un risultato che indica la potenziale presenza di malware in un'istanza Amazon EC2 o in un carico di lavoro di container GuardDuty , avvia automaticamente una scansione del malware senza agenti sui volumi Amazon EBS collegati alla risorsa potenzialmente interessa ta. Per ulteriori informazi oni, consulta GuardDuty	Puoi avviare una scansione antimalware on demand fornendo il nome della risorsa Amazon (ARN) associato all'istanza Amazon EC2 o al carico di lavoro di un container . Puoi avviare una scansione antimalware su richiesta anche quando non viene generato alcun risultato per la tua risorsa. GuardDuty Per ulteriori informazioni, consulta Scansione antimalware on demand.

Factor	GuardDuty-scansione antimalware avviata	Scansione antimalware on demand
	- scansione antimalware avviata.	
Configurazione necessaria	Per utilizzare GuardDuty - initiated malware scan, devi abilitarla per il tuo account. Per ulteriori informazioni, consulta Configurazione della scansione antimalware avviata GuardDuty.	Il tuo account deve essere abilitato GuardDuty . Per utilizzare la scansione antimalware su richiesta, non è richiesta alcuna configura zione a livello di funzionalità.
Tempo di attesa per avviare una nuova scansione	Ogni volta che ne GuardDuty genera unoRisultati che richiamano la scansione GuardDuty antimalware avviata, una scansione antimalware viene avviata automaticamente solo una volta ogni 24 ore.	È possibile avviare una scansione antimalware su richiesta sulla stessa risorsa in qualsiasi momento dopo 1 ora dall'inizio della scansione precedente.
Disponibilità del periodo di prova gratuito di 30 giorni	Quando attivi la scansione antimalware GuardDuty avviata per la prima volta nel tuo account, puoi utilizzare un periodo di prova gratuito di 30 giorni*.	Non è previsto un periodo di prova gratuito* con la scansione antimalware su richiesta per account nuovi o esistenti. GuardDuty

Factor	GuardDuty-scansione antimalware avviata	Scansione antimalware on demand
Opzioni di scansione	Dopo aver configurato la scansione antimalware GuardDuty avviata, Malware Protection ti aiuta anche a selezionare quali risorse scansionare o ignorare. La protezione da malware non avvierà la scansione automatic a delle risorse che scegli di escludere dalla scansione.	La scansione antimalwa re su richiesta supporta un tag globale:. `GuardDuty Excluded` Opzioni di scansione con tag definiti dall'utentenon è applicabile alla scansione antimalware On-demand perché l'ARN della risorsa viene fornito manualmente.

*Dovrai sostenere i costi di utilizzo per la creazione degli snapshot dei volumi EBS e per la conservazione degli snapshot. Per ulteriori informazioni sulla configurazione dell'account per conservare le istantanee, consulta. Conservazione degli snapshot

La protezione da malware è un miglioramento opzionale ed è progettata in modo da non influire sulle prestazioni delle risorse. GuardDuty Per informazioni su come funziona Malware Protection all'interno GuardDuty, consulta. Funzionalità della protezione da malware Per informazioni sulla disponibilità di Malware Protection in diverse Regioni AWS versioni, vedereRegioni ed endpoint.

> **Note**
>
> GuardDuty Malware Protection non supporta Fargate né con Amazon EKS né Amazon ECS.

Funzionalità della protezione da malware

Volume Elastic Block Storage (EBS)

Questa sezione spiega in che modo Malware Protection, inclusa la scansione antimalware GuardDuty avviata e la scansione antimalware su richiesta, analizza i volumi Amazon EBS associati alle istanze Amazon EC2 e ai carichi di lavoro dei container. Prima di procedere, considera le personalizzazioni seguenti:

- Opzioni di scansione: la protezione da malware offre la possibilità di specificare determinati tag per includere o escludere dal processo di scansione particolari istanze Amazon EC2 e volumi Amazon EBS. Solo la scansione antimalware GuardDuty avviata supporta opzioni di scansione con tag definiti dall'utente. Sia la scansione antimalware GuardDuty avviata che la scansione antimalware su richiesta supportano il tag globale. `GuardDutyExcluded` Per ulteriori informazioni, consulta Opzioni di scansione con tag definiti dall'utente.
- Conservazione delle istantanee: Malware Protection offre la possibilità di conservare le istantanee dei volumi Amazon EBS nel tuo account. AWS Per impostazione predefinita, questa opzione è disattivata. Puoi optare per la conservazione delle istantanee sia per le scansioni antimalware GuardDuty avviate che per quelle su richiesta. Per ulteriori informazioni, consulta Conservazione degli snapshot.

Quando viene GuardDuty generato un risultato indicativo della potenziale presenza di malware in un'istanza Amazon EC2 o in un carico di lavoro di container e hai abilitato GuardDuty il tipo di scansione avviata all'interno di Malware Protection, è possibile che venga richiamata GuardDuty una scansione antimalware avviata sulla base delle opzioni di scansione.

Per avviare una scansione antimalware on demand sui volumi Amazon EBS associati a un'istanza Amazon EC2, fornisci il nome della risorsa Amazon (ARN) dell'istanza in questione.

In risposta a una scansione antimalware su richiesta o a una scansione antimalware GuardDuty avviata automaticamente, GuardDuty crea istantanee dei volumi EBS pertinenti collegati alla risorsa potenzialmente interessata e le condivide conGuardDuty account di servizio. Da queste istantanee, GuardDuty crea una replica crittografata del volume EBS nell'account del servizio.

Al termine della scansione, GuardDuty elimina i volumi EBS di replica crittografati e le istantanee dei volumi EBS. Se viene rilevato del malware e hai attivato l'impostazione di conservazione delle istantanee, le istantanee dei tuoi volumi EBS non verranno eliminate e verranno automaticamente conservate nel tuo account. AWS Se non viene rilevato alcun malware, gli snapshot dei volumi EBS non verranno conservati, indipendentemente dall'impostazione di conservazione corrispondente. Per impostazione predefinita, la conservazione degli snapshot è disattivata. Per informazioni sui costi degli snapshot e sulla loro conservazione, consulta Prezzi di Amazon EBS.

GuardDuty conserverà ogni volume EBS di replica nell'account di servizio per un massimo di 55 ore. In caso di interruzione del servizio o di errore con un volume EBS di replica e la relativa scansione antimalware, GuardDuty conserverà tale volume EBS per non più di sette giorni. Il periodo di conservazione prolungato del volume serve a valutare e risolvere l'interruzione o l'errore. GuardDuty

Malware Protection eliminerà i volumi EBS di replica dall'account di servizio dopo aver risolto l'interruzione o l'errore o una volta scaduto il periodo di conservazione prolungato.

Volumi Amazon EBS supportati per la scansione di malware

In tutti i paesi in Regioni AWS cui è GuardDuty supportata la funzionalità Malware Protection, puoi eseguire la scansione dei volumi Amazon EBS non crittografati o crittografati. Puoi avere volumi Amazon EBS crittografati con una delle due chiavi Chiave gestita da AWSo con una chiave gestita dal cliente. Attualmente, alcuni Regioni AWS supportano entrambi i modi di crittografare i volumi Amazon EBS, mentre altri supportano solo chiavi gestite dal cliente.

Per ulteriori informazioni sui casi in cui questa funzionalità non è ancora supportata, consulta China Regions

L'elenco seguente descrive la chiave che GuardDuty utilizza indipendentemente dal fatto che i volumi Amazon EBS siano crittografati o meno:

- Volumi Amazon EBS non crittografati o crittografati con Chiave gestita da AWS: GuardDuty utilizza la propria chiave per crittografare i volumi Amazon EBS di replica.

  Se il tuo account appartiene a una società Regione AWS che non supporta la scansione di volumi Amazon EBS crittografati con l'impostazione predefinita Chiave gestita da AWS per EBS, consulta. Modifica dell'ID AWS KMS chiave predefinito di un volume Amazon EBS
- Volumi Amazon EBS crittografati con chiave gestita dal cliente: GuardDuty utilizza la stessa chiave per crittografare il volume EBS di replica.

Malware Protection non supporta la scansione delle istanze Amazon EC2 con as. `productCode` `marketplace` Se viene avviata una scansione malware per tali istanze Amazon EC2, la scansione verrà ignorata. Per ulteriori informazioni, consulta `UNSUPPORTED_PRODUCT_CODE_TYPE` in Motivi per cui una risorsa viene ignorata durante la scansione malware.

Modifica dell'ID AWS KMS chiave predefinito di un volume Amazon EBS

Per impostazione predefinita, richiamando l'CreateVolumeAPI con crittografia impostata `true` e non specificando l'ID della chiave KMS, viene creato un volume Amazon EBS che viene crittografato con la AWS KMS chiave predefinita per la crittografia EBS. Tuttavia, quando una chiave di crittografia non viene fornita in modo esplicito, puoi modificare la chiave predefinita richiamando l'ModifyEbsDefaultKmsKeyIdAPI o utilizzando il comando corrispondente. AWS CLI

Per modificare l'ID predefinito della chiave EBS, aggiungi la seguente autorizzazione necessaria alla tua policy IAM: `ec2:modifyEbsDefaultKmsKeyId`. Qualsiasi volume Amazon EBS appena creato che scegli di crittografare ma che non specifica un ID chiave KMS associato, utilizzerà l'ID chiave predefinito. Utilizza uno dei seguenti metodi per aggiornare l'ID della chiave predefinita EBS:

Per modificare l'ID predefinito della chiave KMS di un volume Amazon EBS

Esegui una di queste operazioni:

- Utilizzo di un'API: puoi utilizzare l'ModifyEbsDefaultKmsKeyIdAPI. Per informazioni su come visualizzare lo stato di crittografia del volume, consulta Create Amazon EBS volume.
- Utilizzo del AWS CLI comando: l'esempio seguente modifica l'ID chiave KMS predefinito che crittograferà i volumi Amazon EBS se non fornisci un ID chiave KMS. Assicurati di sostituire la regione con l'ID Regione AWS della tua chiave KM.

  ```
  aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-
  id AKIAIOSFODNN7EXAMPLE
  ```

  Il comando precedente genererà un output simile al seguente:

  ```
  {
    "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"
  }
  ```

  Per ulteriori informazioni, vedi modify-ebs-default-kms-key-id.

Personalizzazioni nella protezione da malware

Questa sezione descrive come personalizzare le opzioni di scansione per le istanze Amazon EC2 o i carichi di lavoro dei container quando viene richiamata una scansione antimalware, avviata su richiesta o tramite. GuardDuty

Impostazioni generali

Conservazione degli snapshot

GuardDuty ti offre la possibilità di conservare le istantanee dei tuoi volumi EBS nel tuo account. AWS Per impostazione predefinita, la conservazione degli snapshot è disattivata. Gli snapshot verranno conservati solo se questa impostazione viene attivata prima dell'avvio della scansione.

All'avvio della scansione, GuardDuty genera i volumi EBS di replica in base alle istantanee dei volumi EBS. Una volta completata la scansione e dopo aver già attivato l'impostazione di conservazione degli snapshot nell'account, gli snapshot dei volumi EBS verranno conservati solo in caso di rilevamento di malware e di generazione di Tipi di esiti della protezione da malware. Indipendentemente dal fatto che tu abbia attivato o meno l'impostazione di conservazione delle istantanee, quando non viene rilevato alcun malware, elimina GuardDuty automaticamente le istantanee dei tuoi volumi EBS.

Costo di utilizzo degli snapshot

Durante la scansione antimalware, durante la GuardDuty creazione delle istantanee dei volumi Amazon EBS, a questa fase è associato un costo di utilizzo. Se attivi l'impostazione di conservazione degli snapshot per il tuo account, quando viene rilevato un malware dovrai sostenere i costi di utilizzo per conservare gli snapshot. Per informazioni relative ai costi degli snapshot e alla loro conservazione, consulta Prezzi di Amazon EBS.

Scegli il metodo di accesso che preferisci per attivare l'impostazione di conservazione degli snapshot.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, in Piani di protezione, scegli Protezione da malware.
3. Scegli Impostazioni generali nella sezione inferiore della console. Per conservare gli snapshot, attiva la Conservazione degli snapshot.

API/CLI

1. Esegui UpdateMalwareScanSettingsper aggiornare la configurazione corrente per l'impostazione di conservazione delle istantanee.
2. In alternativa, è possibile eseguire il AWS CLI comando seguente per conservare automaticamente le istantanee quando GuardDuty Malware Protection genera dei risultati.

   Assicurati di sostituire il *`detector-id`* con il tuo `detectorId` valido.
3. Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625554d637e0e4bb3b2 --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

4. Se desideri disattivare la conservazione degli snapshot, sostituisci `RETENTION_WITH_FINDING` con `NO_RETENTION`.

Opzioni di scansione con tag definiti dall'utente

Utilizzando GuardDuty -initiated malware scan, puoi anche specificare tag per includere o escludere le istanze Amazon EC2 e i volumi Amazon EBS dal processo di scansione e rilevamento delle minacce. Puoi personalizzare ogni scansione antimalware GuardDuty avviata modificando i tag nell'elenco dei tag di inclusione o di esclusione. Ogni elenco può includere fino a 50 tag.

Se non disponi già di tag definiti dall'utente associati alle risorse EC2, consulta Tagging delle risorse Amazon EC2 nella Guida per l'utente di Amazon EC2 per le istanze Linux o Tagging delle risorse Amazon EC2 nella Guida per l'utente di Amazon EC2 per le istanze Windows.

> **Note**
>
> La scansione antimalware on demand non supporta le opzioni di scansione con tag definiti dall'utente. Supporta Tag `GuardDutyExcluded` globale.

Per escludere istanze EC2 dalla scansione malware

Se desideri escludere un'istanza Amazon EC2 o un volume Amazon EBS durante il processo di scansione, puoi impostare il `GuardDutyExcluded` tag su qualsiasi istanza Amazon EC2 o volume Amazon EBS e non eseguirai la scansione. `true` GuardDuty Per ulteriori informazioni sul tag `GuardDutyExcluded`, consulta Autorizzazioni del ruolo collegato ai servizi per la protezione da malware. Puoi anche aggiungere un tag di istanza Amazon EC2 a un elenco di esclusione. Se aggiungi più tag all'elenco dei tag di esclusione, qualsiasi istanza Amazon EC2 che contiene almeno uno di questi tag verrà esclusa dal processo di scansione del malware.

Scegli il metodo di accesso che preferisci per aggiungere un tag associato a un'istanza Amazon EC2 a un elenco di esclusione.

Console

1. Apri la console all'indirizzo https://console.aws.amazon.com/guardduty/ GuardDuty .
2. Nel riquadro di navigazione, in Piani di protezione, scegli Protezione da malware.
3. Espandi la sezione Tag di inclusione/esclusione. Scegli Aggiungi tag.
4. Scegli Tag di esclusione, quindi Conferma.
5. Specifica la coppia di **`Key`** e **`Value`** del tag che desideri escludere. Fornire il **`Value`** è facoltativo. Dopo aver aggiunto tutti i tag, scegli Salva.

   > **Important**
   >
   > Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta Limitazioni applicate ai tag nella Guida per l'utente di Amazon EC2 per le istanze Linux o Limitazioni applicate ai tag nella Guida per l'utente di Amazon EC2 per le istanze Windows.

   Se non viene fornito un valore per una chiave e l'istanza EC2 è etichettata con la chiave specificata, questa istanza EC2 verrà esclusa dal processo di scansione antimalware GuardDuty avviato, indipendentemente dal valore assegnato al tag.

API/CLI

- Aggiorna le impostazioni di scansione di malware escludendo un'istanza EC2 o un carico di lavoro di un container dal processo di scansione.

  Il comando di AWS CLI esempio seguente aggiunge un nuovo tag all'elenco dei tag di esclusione. Assicurati di sostituire il *`detector-id`* di esempio con il tuo `detectorId` valido.

  `MapEquals` è un elenco di coppie `Key`/`Value`.

  Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Exclude":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
```

```
"TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
"RETENTION_WITH_FINDING"
```

> **Important**
>
> Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta Limitazioni applicate ai tag nella Guida per l'utente di Amazon EC2 per le istanze Linux o Limitazioni applicate ai tag nella Guida per l'utente di Amazon EC2 per le istanze Windows.

Per includere istanze EC2 nella scansione malware

Se desideri scansionare un'istanza EC2, aggiungi il relativo tag all'elenco di inclusione. Quando aggiungi un tag a un elenco di tag di inclusione, un'istanza EC2 che non contiene nessuno dei tag aggiunti viene ignorata durante la scansione malware. Se aggiungi più tag all'elenco dei tag di inclusione, un'istanza EC2 che contiene almeno uno di questi tag viene inclusa nella scansione malware. A volte, un'istanza EC2 potrebbe essere ignorata durante il processo di scansione. Per ulteriori informazioni, consulta Motivi per cui una risorsa viene ignorata durante la scansione malware.

Scegli il metodo di accesso che preferisci per aggiungere un tag associato a un'istanza EC2 a un elenco di inclusione.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, in Piani di protezione, scegli Protezione da malware.
3. Espandi la sezione Tag di inclusione/esclusione. Scegli Aggiungi tag.
4. Scegli Tag di inclusione, quindi Conferma.
5. Scegli Aggiungi nuovo tag di inclusione e specifica la coppia di **`Key`** e **`Value`** del tag che desideri includere. Fornire il **`Value`** è facoltativo.

   Dopo aver aggiunto tutti i tag di inclusione, scegli Salva.

   Se non viene fornito un valore per una chiave e un'istanza EC2 è contrassegnata con la chiave specificata, tale istanza verrà inclusa nel processo di scansione della protezione da malware, indipendentemente dal valore assegnato al tag.

API/CLI

- Aggiorna le impostazioni di scansione di malware per includere un'istanza EC2 o un carico di lavoro di un container nel processo di scansione.

  Il comando di AWS CLI esempio seguente aggiunge un nuovo tag all'elenco dei tag di inclusione. Assicurati di sostituire il *detector-id* di esempio con il tuo `detectorId` valido. Sostituisci l'esempio *TestKey*e *TestValue*con la `Value` coppia `Key` e del tag associata alla tua risorsa EC2.

  `MapEquals` è un elenco di coppie `Key`/`Value`.

  Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-malware-scan-settings --detector-
  id 60b87779336485625554d637e0e4bb3b2 --scan-resource-criteria '{"Include":
   {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
   "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
   "RETENTION_WITH_FINDING"
  ```

  Important

  Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta Limitazioni applicate ai tag nella Guida per l'utente di Amazon EC2 per le istanze Linux o Limitazioni applicate ai tag nella Guida per l'utente di Amazon EC2 per le istanze Windows.

Note

Potrebbero essere necessari fino a 5 minuti GuardDuty per rilevare un nuovo tag.

In qualsiasi momento, puoi scegliere tra i Tag di inclusione o i Tag di esclusione, ma non entrambi. Se desideri passare da un tag all'altro, sceglilo dal menu a discesa quando aggiungi nuovi tag e Conferma la selezione. Questa operazione cancella tutti i tag correnti.

Tag **`GuardDutyExcluded`** globale

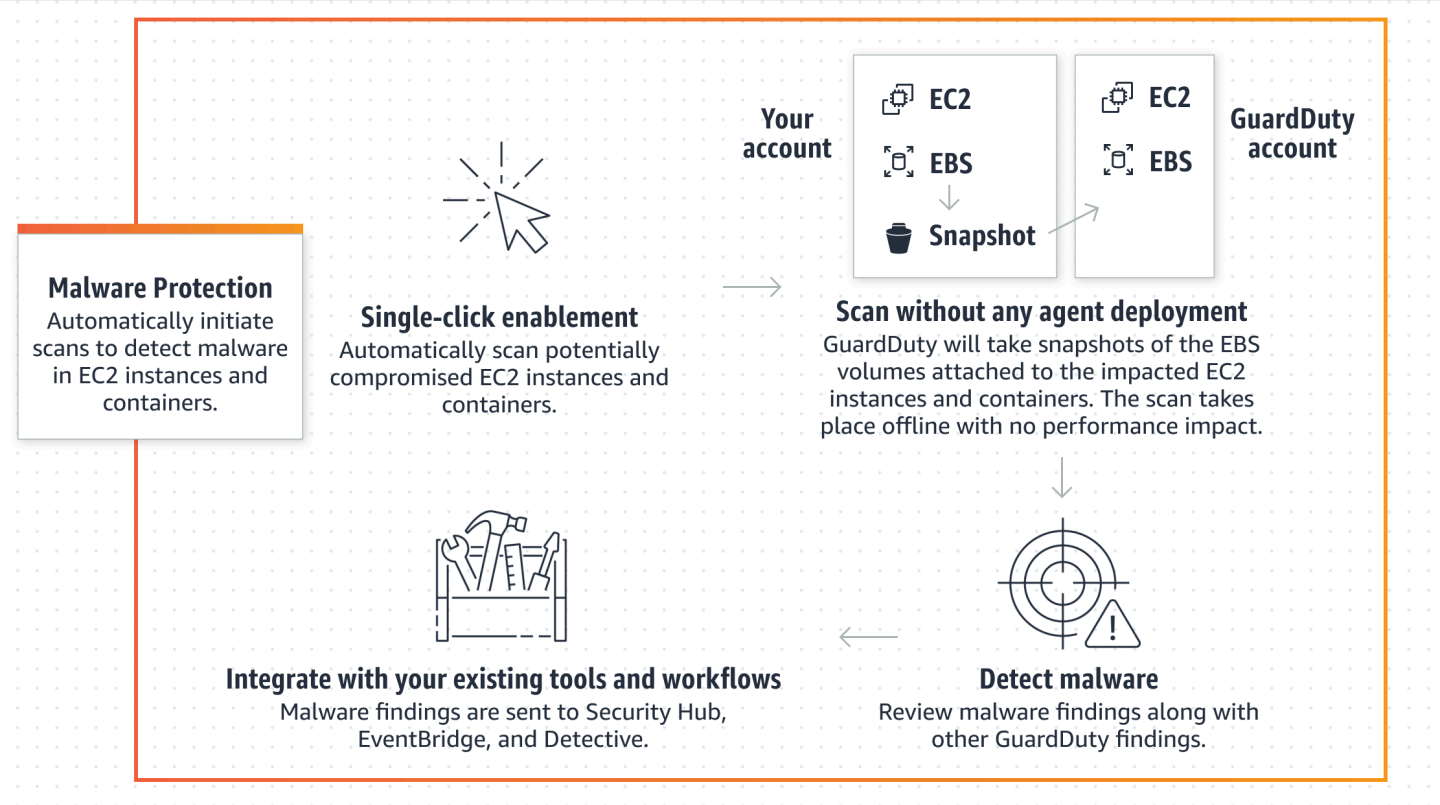
Per impostazione predefinita, gli snapshot dei volumi EBS vengono creati con un tag `GuardDutyScanId`. Non rimuovere questo tag perché così facendo si GuardDuty impedirà l'accesso alle istantanee. Nessuno dei due tipi di scansione della protezione da malware esegue la scansione delle istanze Amazon EC2 o dei volumi Amazon EBS con il tag `GuardDutyExcluded` impostato su `true`. Se tale risorsa viene scansionata della protezione da malware verrà generato un ID di scansione, ma la scansione verrà ignorata indicando un motivo `EXCLUDED_BY_SCAN_SETTINGS`. Per ulteriori informazioni, consulta Motivi per cui una risorsa viene ignorata durante la scansione malware.

GuardDuty- scansione antimalware avviata

Con la scansione antimalware GuardDuty avviata, ogni volta che GuardDuty rileva un'attività dannosa che indica la potenziale presenza di malware nell'istanza Amazon EC2 o nel carico di lavoro del container e GuardDuty generaRisultati che richiamano la scansione GuardDuty antimalware avviata, avvia GuardDuty automaticamente una scansione senza agente sui volumi di Amazon Elastic Block Store (Amazon EBS) collegati all'istanza o al carico di lavoro del container Amazon EC2 potenzialmente interessato per rilevare la presenza di malware. Grazie alle opzioni di scansione, puoi aggiungere tag di inclusione associati alle risorse che desideri scansionare o aggiungere tag di esclusione associati alle risorse che desideri ignorare durante il processo di scansione. L'avvio automatico della scansione terrà sempre sconto delle opzioni di scansione. Puoi anche scegliere di attivare l'impostazione di conservazione degli snapshot per conservare quelli relativi ai volumi EBS solo se la protezione da malware rileva la presenza di malware. Per ulteriori informazioni, consulta Personalizzazioni nella protezione da malware.

Per ogni istanza di Amazon EC2 e carico di lavoro di container per cui vengono GuardDuty generati risultati, viene richiamata una scansione antimalware GuardDuty avviata automaticamente una volta ogni 24 ore. Per informazioni su come vengono scansionati i volumi Amazon EBS collegati all'istanza Amazon EC2 o al carico di lavoro di un container, consulta Funzionalità della protezione da malware.

L'immagine seguente descrive come funziona GuardDuty la scansione antimalware avviata.



Quando viene rilevato un malware, genera. GuardDuty Tipi di esiti della protezione da malware Se GuardDuty non genera un risultato indicativo della presenza di malware sulla stessa risorsa, non verrà richiamata alcuna scansione antimalware GuardDuty avviata. Puoi anche avviare una scansione antimalware on demand sulla stessa risorsa. Per ulteriori informazioni, consulta Scansione antimalware on demand.

In che modo il periodo di prova gratuito di 30 giorni influisce sugli account GuardDuty

Puoi scegliere di attivare o disattivare la funzionalità di scansione antimalware GuardDuty avviata per qualsiasi account o disponibile Regioni AWS, in qualsiasi momento.

- Quando si attiva GuardDuty per la prima volta (nuovo GuardDuty account), la scansione antimalware GuardDuty avviata è già attivata e inclusa nel periodo di prova gratuito di 30 giorni.
- GuardDuty Gli account esistenti possono attivare la scansione antimalware GuardDuty avviata per la prima volta con un periodo di prova gratuito di 30 giorni.
- Se disponi di un GuardDuty account esistente che utilizza Malware Protection prima che la scansione antimalware su richiesta fosse disponibile e tale GuardDuty account utilizza già il modello di prezzo corrispondente Regione AWS, non è necessaria alcuna azione per continuare a utilizzare GuardDuty la scansione antimalware avviata.

> **Note**
>
> Se usufruisci di un periodo di prova gratuito di 30 giorni, continueranno a essere applicati i costi di utilizzo per la creazione degli snapshot dei volumi Amazon EBS e la loro conservazione. Per ulteriori informazioni, consulta Prezzi di Amazon EBS.

Per informazioni sull'attivazione della scansione antimalware GuardDuty avviata dall'utente, consulta. Configurazione della scansione antimalware avviata GuardDuty

Configurazione della scansione antimalware avviata GuardDuty

Configurazione della scansione GuardDuty antimalware avviata per un account indipendente

Per gli account associati a AWS Organizations, è possibile automatizzare questo processo tramite le impostazioni della console, come descritto nella sezione successiva.

Per abilitare o disabilitare la scansione GuardDuty antimalware avviata

Scegli il tuo metodo di accesso preferito per configurare la scansione antimalware GuardDuty avviata per un account autonomo.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, in Piani di protezione, scegli Protezione da malware.
3. Il riquadro Malware Protection elenca lo stato attuale della scansione antimalware GuardDuty avviata per il tuo account. Puoi abilitarla o disabilitarla in qualsiasi momento selezionando rispettivamente Abilita o Disabilita.
4. Selezionare Salva.

API/CLI

- Esegui l'operazione API updateDetector utilizzando il tuo ID rilevatore regionale e impostando l'oggetto `dataSources` con `EbsVolumes` su `true` o `false`.

È inoltre possibile abilitare o disabilitare la scansione anti-malware GuardDuty avviata mediante gli strumenti della riga di AWS comando eseguendo il comando seguente. AWS CLI Assicurati di utilizzare il tuo *ID rilevatore* valido.

> **Note**
>
> Il codice di esempio seguente abilita la scansione antimalware GuardDuty avviata dall'utente. Per disabilitarla, sostituisci `true` con `false`.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

Configurazione della scansione antimalware GuardDuty avviata in ambienti con più account

In un ambiente con più account, solo gli account di GuardDuty amministratore possono configurare la scansione antimalware avviata. GuardDuty GuardDuty gli account amministratore possono abilitare o disabilitare l'uso della scansione antimalware GuardDuty avviata per i rispettivi account membri. Una volta che l'account amministratore ha configurato GuardDuty -initiated malware scan per un account membro, l'account membro seguirà le impostazioni dell'account amministratore e non potrà modificare tali impostazioni tramite la console. GuardDuty gli account amministratore che gestiscono i propri account membri con AWS Organizations supporto possono scegliere di abilitare automaticamente la scansione antimalware GuardDuty avviata su tutti gli account esistenti e nuovi dell'organizzazione. Per ulteriori informazioni, consulta Gestione GuardDuty degli account con AWS Organizations.

Stabilire un accesso affidabile per abilitare la scansione GuardDuty antimalware avviata

Se l'account amministratore GuardDuty delegato non è lo stesso dell'account di gestione dell'organizzazione, l'account di gestione deve abilitare la scansione antimalware GuardDuty avviata dall'organizzazione. In questo modo, l'account amministratore delegato può creare gli account dei membri Autorizzazioni del ruolo collegato ai servizi per la protezione da malware interni gestiti tramite. AWS Organizations

> **Note**
>
> Prima di designare un account GuardDuty amministratore delegato, consulta. Considerazioni e raccomandazioni

Scegliete il metodo di accesso preferito per consentire all'account GuardDuty amministratore delegato di abilitare la scansione antimalware GuardDuty avviata dagli account dei membri dell'organizzazione.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Per accedere, utilizza l'account di gestione della tua AWS Organizations organizzazione.

2. a. Se non hai designato un account GuardDuty amministratore delegato, allora:

      Nella pagina Impostazioni, in Account GuardDuty amministratore delegato, inserisci le 12 cifre **`account ID`** che desideri designare per amministrare la politica nella tua organizzazione. GuardDuty Scegli Delega.

   b. i. Se hai già designato un account GuardDuty amministratore delegato diverso dall'account di gestione, allora:

         Nella pagina Impostazioni, in Amministratore delegato, attiva l'impostazione Autorizzazioni. Questa azione consentirà all'account GuardDuty amministratore delegato di allegare le autorizzazioni pertinenti agli account dei membri e di abilitare la scansione antimalware GuardDuty avviata in tali account membro.

      ii. Se hai già designato un account GuardDuty amministratore delegato uguale all'account di gestione, puoi abilitare direttamente la scansione GuardDuty antimalware avviata per gli account dei membri. Per ulteriori informazioni, consulta Attivazione automatica della scansione antimalware GuardDuty avviata per tutti gli account dei membri.

      > **Tip**
      >
      > Se l'account GuardDuty amministratore delegato è diverso dal tuo account di gestione, devi fornire le autorizzazioni all'account GuardDuty amministratore

delegato per consentire l'attivazione della scansione GuardDuty antimalware avviata per gli account dei membri.

3. Se desideri consentire all'account GuardDuty amministratore delegato di abilitare la scansione antimalware GuardDuty avviata per gli account dei membri in altre regioni, modifica la tua e ripeti i passaggi precedenti. Regione AWS

API/CLI

1. Esegui il comando segunte tramite le credenziali dell'account di gestione:

```
aws organizations enable-aws-service-access --service-principal malware-
protection.guardduty.amazonaws.com
```

2. (Facoltativo) per abilitare la scansione antimalware GuardDuty avviata dall'account di gestione che non è un account amministratore delegato, l'account di gestione la creerà prima Autorizzazioni del ruolo collegato ai servizi per la protezione da malware esplicitamente nel proprio account, quindi abiliterà la scansione antimalware GuardDuty avviata dall'account amministratore delegato, in modo analogo a qualsiasi altro account membro.

```
aws iam create-service-linked-role --aws-service-name malware-
protection.guardduty.amazonaws.com
```

3. L'account amministratore delegato è stato designato nell'account attualmente selezionato GuardDuty . Regione AWS Se hai designato un account come account GuardDuty amministratore delegato in una regione, quell'account deve essere il tuo account GuardDuty amministratore delegato in tutte le altre regioni. Ripeti la fase precedente per tutte le altre regioni.

Configurazione della scansione GuardDuty antimalware avviata per l'account amministratore delegato GuardDuty

Scegliete il metodo di accesso preferito per abilitare o disabilitare la scansione antimalware GuardDuty avviata per un account amministratore delegato. GuardDuty

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

Assicurati di utilizzare le credenziali dell'account di gestione.

2. Nel riquadro di navigazione, scegli Protezione da malware.
3. Nella pagina Protezione da malware, scegli Modifica accanto a GuardDuty-initiated malware scan.
4. Esegui una di queste operazioni:

   Utilizzando Abilita per tutti gli account

   - Scegli Abilita per tutti gli account. Ciò abiliterà il piano di protezione per tutti gli GuardDuty account attivi nell' AWS organizzazione, inclusi i nuovi account che entrano a far parte dell'organizzazione.
   - Selezionare Salva.

   Utilizzando Configura gli account manualmente

   - Per abilitare il piano di protezione solo per l'account GuardDuty amministratore delegato, scegli Configura gli account manualmente.
   - Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).
   - Selezionare Salva.

API/CLI

Esegui l'operazione API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il `name` dell'oggetto `features` su `EBS_MALWARE_PROTECTION` e lo `status` su `ENABLED` o `DISABLED`.

È possibile abilitare o disabilitare GuardDuty -initiated malware scan eseguendo il seguente comando. AWS CLI *`Assicurati di utilizzare l'ID rilevatore valido GuardDuty dell'account amministratore delegato.`*

> **Note**
>
> Il codice di esempio seguente abilita la scansione antimalware GuardDuty avviata dall'utente. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /
              --account-ids 555555555555 /
              --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Attivazione automatica della scansione antimalware GuardDuty avviata per tutti gli account dei membri

Scegli il metodo di accesso preferito per abilitare la funzionalità di scansione antimalware GuardDuty avviata per tutti gli account membri. inclusi gli account membri esistenti e i nuovi account che entrano a far parte dell'organizzazione.

Console

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una di queste operazioni:

   Utilizzando la pagina Protezione da malware

   1. Nel riquadro di navigazione, scegli Protezione da malware.
   2. Nella pagina Protezione da malware, scegli Modifica nella sezione GuardDuty -initiated malware scan.
   3. Scegli Abilita per tutti gli account. Questa azione abilita automaticamente la scansione antimalware GuardDuty avviata sia per gli account esistenti che per quelli nuovi dell'organizzazione.
   4. Selezionare Salva.

   > **Note**
   >
   > L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Utilizzando la pagina Account

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
3. Nella finestra Gestisci le preferenze di attivazione automatica, scegli Abilita per tutti gli account sottoposti alla scansione GuardDutyantimalware avviata.
4. Nella pagina Protezione da malware, scegli Modifica nella sezione GuardDuty -initiated malware scan.
5. Scegli Abilita per tutti gli account. Questa azione abilita automaticamente la scansione antimalware GuardDuty avviata sia per gli account esistenti che per quelli nuovi dell'organizzazione.
6. Selezionare Salva.

> **Note**
>
> L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Utilizzando la pagina Account

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
3. Nella finestra Gestisci le preferenze di attivazione automatica, scegli Abilita per tutti gli account sottoposti alla scansione GuardDutyantimalware avviata.
4. Selezionare Salva.

Se non puoi utilizzare l'opzione Abilita per tutti gli account, consulta Abilita o disabilita in modo selettivo la scansione antimalware GuardDuty avviata dagli account dei membri.

API/CLI

- *Per abilitare o disabilitare in modo selettivo la scansione antimalware GuardDuty avviata per i tuoi account membri, richiama l'operazione updateMemberDetectorsAPI utilizzando il tuo ID di rilevamento.*
- L'esempio seguente mostra come abilitare la scansione antimalware GuardDuty avviata da un singolo account membro. Per disabilitare un account membro, sostituisci `ENABLED` con `DISABLED`.

  Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

  Puoi anche trasmettere un elenco di ID account separati da uno spazio.
- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilita la scansione antimalware GuardDuty avviata per tutti gli account dei membri attivi esistenti

Scegliete il metodo di accesso preferito per abilitare la scansione antimalware GuardDuty avviata per tutti gli account dei membri attivi esistenti nell'organizzazione.

Per configurare la scansione antimalware GuardDuty avviata per tutti gli account dei membri attivi esistenti

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.
2. Nel riquadro di navigazione, scegli Protezione da malware.
3. In Malware Protection, è possibile visualizzare lo stato corrente della configurazione di scansione GuardDutyantimalware avviata. Nella sezione Account membri attivi, scegli Operazioni.

4. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
5. Selezionare Salva.

Attiva automaticamente la scansione GuardDuty antimalware avviata per gli account dei nuovi membri

Gli account membri appena aggiunti devono essere abilitati GuardDuty prima di selezionare la configurazione GuardDuty della scansione antimalware avviata. Gli account membri gestiti su invito possono configurare manualmente la scansione antimalware GuardDuty avviata per i propri account. Per ulteriori informazioni, consulta Step 3 - Accept an invitation.

Scegliete il metodo di accesso preferito per abilitare la scansione antimalware GuardDuty avviata dai nuovi account che entrano a far parte della vostra organizzazione.

Console

L'account GuardDuty amministratore delegato può abilitare la scansione antimalware GuardDuty avviata per gli account di nuovi membri di un'organizzazione, utilizzando la pagina Malware Protection o Account.

Per abilitare automaticamente la scansione antimalware GuardDuty avviata per i nuovi account dei membri

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.
2. Esegui una di queste operazioni:
   - Utilizzando la pagina Protezione da malware:
     1. Nel riquadro di navigazione, scegli Protezione da malware.
     2. Nella pagina Protezione da malware, scegli Modifica nella scansione GuardDuty antimalware avviata.
     3. Scegli Configura gli account manualmente.
     4. Seleziona Abilita automaticamente per i nuovi account membri. Questo passaggio garantisce che ogni volta che un nuovo account si unisce alla tua organizzazione, la scansione antimalware GuardDuty avviata venga automaticamente abilitata per tale account. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa configurazione.

5. Selezionare Salva.

- Utilizzando la pagina Account:

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica.
3. Nella finestra Gestisci le preferenze di attivazione automatica, seleziona Abilita per nuovi account nella sezione GuardDuty-initiated malware scan.
4. Selezionare Salva.

API/CLI

- *Per abilitare o disabilitare la scansione antimalware GuardDuty avviata per i nuovi account membri, richiama l'operazione UpdateOrganizationConfigurationAPI utilizzando il tuo ID di rilevamento.*
- L'esempio seguente mostra come abilitare la scansione antimalware GuardDuty avviata da un singolo account membro. Per disabilitarlo, consulta Abilita o disabilita in modo selettivo la scansione antimalware GuardDuty avviata dagli account dei membri. Se non desideri abilitarlo per tutti i nuovi account che entrano a far parte dell'organizzazione, imposta `AutoEnable` su `NONE`.

  Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

  Puoi anche trasmettere un elenco di ID account separati da uno spazio.
- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilita o disabilita in modo selettivo la scansione antimalware GuardDuty avviata dagli account dei membri

Scegli il tuo metodo di accesso preferito per configurare selettivamente la scansione antimalware GuardDuty avviata per gli account dei membri.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Nella pagina Account, controlla lo stato del tuo account membro nella colonna GuardDuty-initiated malware scan.
4. Seleziona l'account per il quale desideri configurare GuardDuty -initiated malware scan. Puoi selezionare più account alla volta.
5. Dal menu Modifica piani di protezione, scegli l'opzione appropriata per GuardDuty-initiated malware scan.

API/CLI

Per abilitare o disabilitare in modo selettivo la scansione antimalware GuardDuty avviata per i tuoi account membri, richiama l'operazione updateMemberDetectorsAPI utilizzando il tuo ID di rilevamento.

L'esempio seguente mostra come abilitare la scansione antimalware GuardDuty avviata da un singolo account membro. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

> **Note**
>
> Puoi anche trasmettere un elenco di ID account separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Per abilitare o disabilitare in modo selettivo la scansione antimalware GuardDuty avviata dagli account dei membri, esegui l'operazione [updateMemberDetectors](#)API utilizzando il tuo ID di rilevamento. L'esempio seguente mostra come abilitare la scansione antimalware GuardDuty avviata da un solo utente. Per disabilitarla, sostituisci `true` con `false`.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 123456789012 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

> **Note**
>
> Puoi anche trasmettere un elenco di ID account separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilita la scansione antimalware GuardDuty avviata per gli account esistenti nell'organizzazione gestiti tramite invito

Il ruolo collegato al servizio GuardDuty Malware Protection (SLR) deve essere creato negli account dei membri. L'account amministratore non può abilitare la funzionalità di scansione antimalware GuardDuty avviata da. AWS Organizations

Attualmente, è possibile eseguire le seguenti operazioni tramite la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/ per abilitare la scansione antimalware GuardDuty avviata dagli account dei membri esistenti.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando le credenziali del tuo account amministratore.
2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Seleziona l'account membro per il quale desideri abilitare la scansione GuardDuty antimalware avviata. Puoi selezionare più account alla volta.
4. Scegli Azioni.
5. Scegli Disassocia membro.
6. Nel tuo account membro, nel riquadro di navigazione, scegli Protezione da malware in Piani di protezione.
7. Scegli Abilita la scansione GuardDuty antimalware avviata. GuardDuty creerà una reflex per l'account del membro. Per ulteriori informazioni sul ruolo collegato ai servizi, consulta Autorizzazioni del ruolo collegato ai servizi per la protezione da malware.
8. Nel tuo account amministratore, scegli Account nel pannello di navigazione.
9. Scegli l'account membro da aggiungere nuovamente all'organizzazione.
10. Scegli Operazioni, quindi Aggiungi membro.

API/CLI

1. Utilizza l'account amministratore per eseguire l'DisassociateMembersAPI sugli account dei membri che desiderano abilitare la scansione GuardDuty antimalware avviata.
2. Usa il tuo account membro per invocare e UpdateDetectorabilitare la scansione GuardDuty antimalware avviata.

   Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

   ```
   aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
   {"EbsVolumes":true}}}'
   ```
3. Utilizza l'account amministratore per eseguire l'CreateMembersAPI per aggiungere nuovamente il membro all'organizzazione.

Risultati che richiamano la scansione GuardDuty antimalware avviata

Una scansione antimalware GuardDuty avviata viene richiamata quando GuardDuty rileva comportamenti sospetti indicativi di malware su istanze Amazon EC2 o carichi di lavoro in container.

- 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
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce (solo in uscita)
- 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 (solo in uscita)
- UnauthorizedAccess:EC2/SSHBruteForce (solo in uscita)
- 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

Scansione antimalware on demand

La scansione antimalware on demand è utile per rilevare la presenza di malware sui volumi Amazon Elastic Block Store (Amazon EBS) collegati alle istanze Amazon EC2. Senza necessità di configurazione, puoi avviare una scansione antimalware on demand fornendo il nome della risorsa Amazon (ARN) dell'istanza Amazon EC2 che desideri scansionare. Puoi avviare una scansione antimalware su richiesta tramite la console o l'API. GuardDuty Prima di avviare una scansione antimalware on demand, puoi impostare l'impostazione di Conservazione degli snapshot che preferisci. I seguenti scenari possono aiutarti a identificare quando utilizzare il tipo di scansione antimalware On-demand con: GuardDuty

- Vuoi rilevare la presenza di malware nelle tue istanze Amazon EC2 senza abilitare la scansione GuardDuty antimalware avviata.
- Hai abilitato la scansione antimalware GuardDuty avviata e una scansione è stata richiamata automaticamente. Dopo aver eseguito la correzione consigliata per il tipo di esito generato dalla protezione da malware, se desideri avviare una scansione sulla stessa risorsa, puoi avviare una scansione antimalware on demand dopo che è trascorsa 1 ora dall'inizio di quella precedente.

  Per la scansione antimalware on demand non è necessario che siano trascorse 24 ore dal momento in cui è stata avviata la scansione precedente. Deve trascorrere 1 ora prima di avviare una scansione antimalware on demand sulla stessa risorsa. Per evitare di duplicare una scansione malware sulla stessa istanza EC2, consulta Esecuzione di una nuova scansione della stessa istanza Amazon EC2.

> **Note**
>
> La scansione antimalware su richiesta non è inclusa nel periodo di prova gratuito di 30 giorni con. GuardDuty Il costo di utilizzo si applica al volume totale di Amazon EBS scansionato per ogni scansione malware. Per ulteriori informazioni, consulta i GuardDuty prezzi di Amazon. Per informazioni sui costi relativi alla creazione e alla conservazione degli snapshot dei volumi Amazon EBS, consulta Prezzi di Amazon EBS.

Come funziona la scansione antimalware on demand

Con la scansione antimalware on demand, puoi avviare una richiesta di scansione antimalware per l'istanza Amazon EC2 anche mentre è in uso. Dopo aver avviato una scansione antimalware su

richiesta, GuardDuty crea istantanee dei volumi Amazon EBS collegati all'istanza Amazon EC2 il cui Amazon Resource Name (ARN) è stato fornito per la scansione. Successivamente, condivide queste istantanee con GuardDuty . GuardDuty account di servizio GuardDuty crea volumi EBS di replica crittografati da tali istantanee nell'account del servizio. GuardDuty Per ulteriori informazioni su come vengono scansionati i volumi Amazon EBS, consulta Volume Elastic Block Storage (EBS).

> **Note**
>
> GuardDuty crea le istantanee dei dati che sono già stati scritti nei volumi Amazon EBS al momento dell' point-in-time avvio di una scansione antimalware su richiesta.

Se viene rilevato un malware e hai abilitato l'impostazione di conservazione degli snapshot, gli snapshot del volume EBS vengono automaticamente conservati nel tuo Account AWS. La scansione antimalware on demand genera Tipi di esiti della protezione da malware. Se non viene rilevato alcun malware, indipendentemente dall'impostazione di conservazione, gli snapshot dei volumi EBS vengono eliminati.

Per impostazione predefinita, gli snapshot dei volumi EBS vengono creati con un tag `GuardDutyScanId`. Non rimuovere questo tag perché così facendo si GuardDuty impedirà l'accesso alle istantanee. Nessuno dei due tipi di scansione della protezione da malware esegue la scansione delle istanze Amazon EC2 o dei volumi Amazon EBS con il tag `GuardDutyExcluded` impostato su `true`. Se tale risorsa viene scansionata della protezione da malware verrà generato un ID di scansione, ma la scansione verrà ignorata indicando un motivo `EXCLUDED_BY_SCAN_SETTINGS`. Per ulteriori informazioni, consulta Motivi per cui una risorsa viene ignorata durante la scansione malware.

AWS Organizations politica di controllo del servizio: accesso negato

Utilizzando le policy di controllo del servizio (SCP) in AWS Organizations, l'account GuardDuty amministratore delegato può limitare le autorizzazioni e negare azioni come l'avvio di una scansione antimalware su richiesta per l'istanza Amazon EC2 di proprietà dei tuoi account.

Come account GuardDuty membro, quando avvii una scansione antimalware su richiesta per le tue istanze Amazon EC2, potresti ricevere un errore. Puoi connetterti all'account di gestione per capire il motivo per cui è stata configurata una SCP per il tuo account membro. Per ulteriori informazioni, consulta Effetti delle SCP sulle autorizzazioni.

Nozioni di base sulla scansione antimalware on demand

In qualità di account GuardDuty amministratore, puoi avviare una scansione antimalware su richiesta per conto dei tuoi account membri attivi che hanno i seguenti prerequisiti impostati nei rispettivi account. Gli account autonomi e gli account membro attivi GuardDuty possono anche avviare una scansione antimalware su richiesta per le proprie istanze Amazon EC2.

Prerequisiti

- GuardDuty deve essere abilitato nel punto in Regioni AWS cui desideri avviare la scansione antimalware su richiesta.
- Assicurati che sia presente il collegamento tra AWS politica gestita: AmazonGuardDutyFullAccess e l'utente IAM o il ruolo IAM. Avrai bisogno della chiave di accesso e della chiave segreta associate all'utente IAM o al ruolo IAM.
- In qualità di account GuardDuty amministratore delegato, hai la possibilità di avviare una scansione antimalware su richiesta per conto di un account membro attivo.
- Se sei un account membro senza Autorizzazioni del ruolo collegato ai servizi per la protezione da malware, l'avvio di una scansione antimalware on demand per un'istanza Amazon EC2 appartenente al tuo account creerà automaticamente l'SLR per la protezione da malware.

> **Important**
>
> Assicurati che nessuno elimini le autorizzazioni SLR per Malware Protection quando la scansione antimalware, GuardDuty avviata o su richiesta, è ancora in corso. Ciò impedirebbe il corretto completamento della scansione e comprometterebbe la precisione dell'esito.

Prima di avviare una scansione antimalware on demand, assicurati che non sia stata avviata alcuna scansione sulla stessa risorsa nell'ultima ora, altrimenti verrà duplicata. Per ulteriori informazioni, consulta Esecuzione di una nuova scansione della stessa risorsa.

Avvio della scansione antimalware on demand

Scegli il metodo di accesso che preferisci per avviare una scansione antimalware on demand.

Console

1. Apri la console all'indirizzo https://console.aws.amazon.com/guardduty/. GuardDuty

2. Avvia la scansione utilizzando una delle opzioni seguenti:

   a. Utilizzando la pagina Protezione da malware:

      i. Nel riquadro di navigazione, in Piani di protezione, scegli Protezione da malware.

      ii. Nella pagina Protezione da malware, fornisci l'ARN dell'istanza Amazon EC2[1] per la quale desideri avviare la scansione.

   b. Utilizzando la pagina Scansioni malware:

      i. Nel riquadro di navigazione, scegli Scansioni malware.

      ii. Scegli Avvia scansione on demand e fornisci l'ARN dell'istanza Amazon EC2[1] per cui desideri avviare la scansione.

      iii. Se si tratta di una nuova scansione, seleziona un ID istanza Amazon EC2 nella pagina Scansioni malware.

      Espandi il menu a discesa Avvia scansione on demand e scegli Esegui nuovamente la scansione dell'istanza selezionata.

3. Dopo aver avviato correttamente una scansione utilizzando uno dei due metodi, viene generato un ID che può essere utilizzato per tenere traccia dello stato di avanzamento della scansione. Per ulteriori informazioni, consulta Monitoraggio dello stato e del risultato delle scansioni malware.

API/CLI

Invoke StartMalwareScanthat accetta l'istanza[1] `resourceArn` di Amazon EC2 per la quale desideri avviare una scansione antimalware su richiesta.

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-
east-1:555555555555:instance/i-b188560f"
```

Dopo aver avviato correttamente una scansione, `StartMalwareScan` restituisce uno `scanId`. Invoke DescribeMalwareScansmonitora l'avanzamento della scansione avviata.

[1]Per informazioni sul formato dell'ARN dell'istanza Amazon EC2, consulta Nome della risorsa Amazon (ARN). Per le istanze Amazon EC2, puoi utilizzare il seguente formato ARN di esempio sostituendo i valori per la partizione, la regione, l'ID Account AWS e l'ID dell'istanza Amazon EC2. Per informazioni sulla lunghezza dell'ID dell'istanza, consulta ID risorsa.

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

Esecuzione di una nuova scansione della stessa istanza Amazon EC2

Indipendentemente dal fatto che una scansione sia GuardDuty avviata o su richiesta, puoi avviare una nuova scansione antimalware su richiesta sulla stessa istanza EC2 dopo 1 ora dall'inizio della scansione antimalware precedente. Se la nuova scansione malware viene avviata entro 1 ora dall'avvio della scansione antimalware precedente, la richiesta genererà il seguente errore e non verrà generato alcun ID di scansione.

```
A scan was initiated on this resource recently. You can request a scan on
the same resource one hour after the previous scan start time.
```

Per informazioni su come avviare una nuova scansione sulla stessa risorsa, consulta Avvio della scansione antimalware on demand.

Per monitorare lo stato delle scansioni malware, consulta Monitoraggio degli stati e dei risultati della scansione in Malware Protection GuardDuty .

Monitoraggio degli stati e dei risultati della scansione in Malware Protection GuardDuty

È possibile monitorare lo stato di scansione di ogni scansione di GuardDuty Malware Protection. I valori possibili per lo Stato delle scansioni sono `Completed`, `Running`, `Skipped` e `Failed`.

Al termine della scansione, il Risultato della scansione viene compilato per le scansioni con lo Stato corrispondente a `Completed`. I valori possibili per il Risultato della scansione sono `Clean` e `Infected`. Tramite il Tipo di scansione, puoi identificare se la scansione malware era `GuardDuty initiated` or `On demand`.

I risultati di ogni scansione malware vengono conservati per 90 giorni. Scegli il metodo di accesso che preferisci per monitorare lo stato della scansione malware.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Scansioni malware.

3. Puoi filtrare le scansioni malware in base alle seguenti Proprietà disponibili nei criteri di filtro.

   - ID scansione
   - ID account
   - ARN dell'istanza EC2
   - Tipo di scansione
   - Stato della scansione

   Per informazioni sulle proprietà utilizzate per i criteri di filtro, consulta Dettagli degli esiti.

API/CLI

- Dopo che la scansione ha prodotto un risultato, puoi filtrare le scansioni malware sulla base di `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE` `GUARDDUTY_FINDING_ID`, `SCAN_STATUS` e `SCAN_START_TIME`.

  I criteri di `GUARDDUTY_FINDING_ID` filtro sono disponibili quando `SCAN_TYPE` viene GuardDuty avviato. Per informazioni su qualsiasi criterio di filtro, consulta Dettagli degli esiti.
- Puoi modificare i *`filter-criteria`* di esempio nel comando seguente. Attualmente, puoi applicare filtri utilizzando una `CriterionKey` alla volta. Le opzioni per la `CriterionKey` sono `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE` `GUARDDUTY_FINDING_ID`, `SCAN_STATUS` e `SCAN_START_TIME`.

  Se usi la stessa `CriterionKey` riportata di seguito, assicurati di sostituire `EqualsValue` di esempio con il tuo *`scan-id`* AWS valido.

  Sostituisci il `detector-id` di esempio con il tuo *`detector-id`* valido. Puoi modificare il numero di *`max-results`* (fino a 50) e *`sort-criteria`*. Il `AttributeName` è obbligatorio e deve essere `scanStartTime`.

  ```
  aws guardduty describe-malware-scans --detector-
  id 60b87779336485625 54d637e0e4bb3b2 --max-results 1 --sort-criteria
   '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
   '{"FilterCriterion":[{"CriterionKey":"SCAN_ID", "FilterCondition":
  {"EqualsValue":"123456789012"}}] }'
  ```
- La risposta di questo comando mostra al massimo un risultato contenente i dettagli sulla risorsa interessata e sugli esiti relativi ai malware (se `Infected`).

GuardDuty account di servizio di Regione AWS

Quando un'istantanea viene creata e condivisa con un account di GuardDuty servizio, nei CloudTrail registri viene creato un nuovo evento. Questo evento specifica l'`snapshotId`and `userId` (account di GuardDuty servizio corrispondente). Regione AWS Per ulteriori informazioni, consulta Funzionalità della protezione da malware.

L'esempio seguente è un frammento di un CloudTrail evento che mostra il corpo della richiesta: `ModifySnapshotAttribute`

```
"requestParameters": {
        "snapshotId": "snap-1234567890abcdef0",
        "createVolumePermission": {
            "add": {
                "items": [
                    {
                        "userId": "111122223333"
                    }
                ]
            }
        },
        "attributeType": "CREATE_VOLUME_PERMISSION"
    }
```

La tabella seguente mostra gli account GuardDuty di servizio per ogni regione. `userId`È l'account del GuardDuty servizio e dipende dalla regione selezionata.

Regione AWS	Codice regione	GuardDuty ID dell'account di servizio (**`userId`**)
Stati Uniti orientali (Virginia settentrionale)	us-east-1	652050842985
Stati Uniti orientali (Ohio)	us-east-2	178123968615
Stati Uniti occidentali (California settentrionale)	us-west-1	669213148797
US West (Oregon)	us-west-2	447226417196

Regione AWS	Codice regione	GuardDuty ID dell'account di servizio (**`userId`**)
Asia Pacifico (Mumbai)	ap-south-1	913179291432
Asia Pacifico (Osaka-Locale)	ap-northeast-3	089661699081
Asia Pacifico (Seul)	ap-northeast-2	039163547507
Asia Pacifico (Tokyo)	ap-northeast-1	874749492622
Asia Pacifico (Singapore)	ap-southeast-1	247460962669
Asia Pacifico (Sydney)	ap-southeast-2	124839743349
Canada (Centrale)	ca-central-1	175877067165
Canada occidentale (Calgary)	ca-west-1	894794104037
Europa (Francoforte)	eu-central-1	002294850712
Europa (Irlanda)	eu-west-1	283769539786
Europa (Londra)	eu-west-2	310125036783
Europa (Parigi)	eu-west-3	866607715269
Europa (Stoccolma)	eu-north-1	693780578038
Cina (Pechino)	cn-north-1	448721096076
Cina (Ningxia)	cn-northwest-1	480864352451
Sud America (San Paolo)	sa-east-1	546914126324
Asia Pacifico (Hyderabad) (con consenso esplicito)	ap-south-2	682251015962

Regione AWS	Codice regione	GuardDuty ID dell'account di servizio (**`userId`**)
Asia Pacifico (Melbourne) (con consenso esplicito)	ap-southeast-4	353488359550
Europa (Spagna) (con consenso esplicito)	eu-south-2	936182149045
Europa (Zurigo) (con consenso esplicito)	eu-central-2	867642063380
Israele (Tel Aviv) (con consenso esplicito)	il-central-1	619233833001
Europa (Milano) (con consenso esplicito)	eu-south-1	977238331021
Asia Pacifico (Hong Kong) (con consenso esplicito)	ap-east-1	249472122084
Medio Oriente (Bahrein) (con consenso esplicito)	me-south-1	404001805210
Africa (Città del Capo) (con consenso esplicito)	af-south-1	957664736811
Asia Pacifico (Giacarta) (con consenso esplicito)	ap-southeast-3	452118225523
Medio Oriente (EAU) (con consenso esplicito)	me-central-1	828603743433

Quote di protezione da malware

La protezione da malware ha la seguente disponibilità predefinita delle varie risorse che la funzionalità utilizza.

Ambito	Predefinita	Commenti
Estrazione e analisi dei dati in file compressi o archiviati	5	Il numero massimo di livelli nidificati consentiti in un file archiviato.
Numero di file all'interno di un file archiviato	1000	Il numero massimo di file che possono essere scansiona ti all'interno di un archivio. Questo conteggio è la somma del numero di file estratti dall'archivio e del numero di file estratti da tutti gli archivi annidati.
Numero delle minacce	32	Il numero massimo di minacce che è possibile visualizzare nel pannello dei risultati. GuardDuty Malware Protectio n potrebbe aver rilevato più nomi di minacce. Se il numero di nomi di minacce rilevate è superiore al valore predefinito, puoi visualizzare i dettagli JSON selezionando l'ID di ricerca sotto il nome del risultato nel pannello dei dettagli della GuardDuty console.
Numero di file per minaccia rilevata	5	Il numero massimo di file identificati per ogni minaccia rilevata. Ad esempio, se GuardDuty rileva 10 file associati a una singola minaccia, la minaccia mostrerà un massimo di 5 file.

Ambito	Predefinita	Commenti
Volumi EBS per ogni scansione di ogni istanza	11	Il numero massimo di volumi EBS che GuardDuty possono essere scansionati per istanza EC2. Se ci sono più di 11 volumi EBS da scansionare, GuardDuty Malware Protection li ordina `deviceName` alfabeticamente e seleziona i primi 11 volumi EBS.
Dimensione del volume EBS	1024 GB	La dimensione massima del volume EBS in GB che Malware Protection può scansionare in ciascuna regione GuardDuty .
Tipi di file system supportati	GuardDuty Malware Protection può scansionare i seguenti tipi di file system: • New Technology File System (NTFS) • X File System (XFS) • File System second extended (ext2) • File System fourth extended (ext4) • File system File Allocation Table (FAT) • File system Virtual File Allocation Table (VFAT)	N/D.

Ambito	Predefinita	Commenti
Tag delle opzioni di scansione	50	Il numero massimo dei tag delle risorse che puoi aggiungere per personalizzare l'impostazione delle opzioni di scansione malware. Per ulteriori informazioni, consulta Opzioni di scansione con tag definiti dall'utente.
Ritrovamento del periodo di conservazione	90	Il numero massimo di giorni in cui viene GuardDuty conservato un risultato. Per le informazioni più recenti, consulta Quote per Amazon GuardDuty.
Periodo di conservazione delle scansioni malware	90	Il numero massimo di giorni in cui GuardDuty Malware Protection conserva la cronologia di una scansione. Per ulteriori informazioni sulla visualizzazione delle scansioni malware recenti, consulta Monitoraggio degli stati e dei risultati della scansione in Malware Protection GuardDuty .
Transazioni al secondo (TPS) per la scansione antimalware on demand	1	Il numero di richieste di scansione antimalware on demand che possono essere avviate al secondo in ciascuna regione.

Ambito	Predefinita	Commenti
Limite di burst per la scansione antimalware on demand	1	Il numero di richieste simultanee di scansione antimalware on demand che possono essere avviate al secondo in ciascuna regione.

GuardDuty Protezione RDS

RDS Protection in Amazon GuardDuty analizza e profila l'attività di accesso RDS per potenziali minacce di accesso ai database Amazon Aurora (Amazon Aurora MySQL Compatible Edition e Aurora PostgreSQL Compatible Edition). La funzionalità consente di identificare comportamenti di accesso potenzialmente sospetti. La Protezione RDS non richiede un'infrastruttura aggiuntiva ed è progettata in modo da non influire negativamente sulle prestazioni delle istanze di database.

Quando RDS Protection rileva un tentativo di accesso potenzialmente sospetto o anomalo che indica una minaccia per il database, genera una nuova scoperta con dettagli sul database potenzialmente compromesso. GuardDuty

Puoi abilitare o disabilitare la funzionalità RDS Protection per qualsiasi account in qualsiasi Regione AWS luogo in cui questa funzione è disponibile in Amazon GuardDuty, in qualsiasi momento. Un GuardDuty account esistente può abilitare RDS Protection con un periodo di prova di 30 giorni. Per un nuovo GuardDuty account, RDS Protection è già abilitato e incluso nel periodo di prova gratuito di 30 giorni. Per ulteriori informazioni, consulta Stima del costo.

> **Note**
>
> Quando la funzionalità RDS Protection non è abilitata, non raccoglie le attività di accesso RDS GuardDuty né rileva comportamenti di accesso anomali o sospetti.

Per informazioni su Regioni AWS dove GuardDuty non supporta ancora la protezione RDS, consulta. Disponibilità di funzionalità specifiche per ogni regione

Database Amazon Aurora supportati

La tabella seguente mostra le versioni del database Aurora supportate.

Motore database Amazon Aurora	Versioni del motore supportate
Aurora MySQL	• 2.10.2 o versioni successive • 3.02.1 o versioni successive
Aurora PostgreSQL	• 10.17 o versioni successive

Motore database Amazon Aurora	Versioni del motore supportate
	• 11.12 o versioni successive • 12.7 o versioni successive • 13.3 o versioni successive • 14.3 o versioni successive • 15.2 o versione successiva • 16.1 o versione successiva

Come la Protezione RDS utilizza il monitoraggio delle attività di accesso RDS

RDS Protection in Amazon ti GuardDuty aiuta a proteggere i database Amazon Aurora (Aurora) supportati nel tuo account. Dopo aver abilitato la funzionalità RDS Protection, inizia GuardDuty immediatamente a monitorare l'attività di accesso RDS dai database Aurora del tuo account. GuardDuty monitora e profila continuamente l'attività di accesso RDS per attività sospette, ad esempio l'accesso non autorizzato al database Aurora nel tuo account, da parte di un attore esterno invisibile in precedenza. Quando abiliti la Protezione RDS per la prima volta o hai un'istanza di database appena creata, è necessario un periodo di apprendimento per definire il comportamento normale. Per questo motivo, alle istanze di database appena abilitate o appena create potrebbero non essere associati esiti relativi a un accesso anomalo per un massimo di due settimane. Per ulteriori informazioni, consulta Monitoraggio delle attività di accesso RDS.

Quando RDS Protection rileva una potenziale minaccia, ad esempio uno schema insolito in una serie di tentativi di accesso riusciti, falliti o incompleti, GuardDuty genera una nuova scoperta con dettagli sull'istanza di database potenzialmente compromessa. Per ulteriori informazioni, consulta Tipi di esiti della Protezione RDS. Se disabiliti RDS Protection, interrompe GuardDuty immediatamente il monitoraggio dell'attività di accesso RDS e non è in grado di rilevare alcuna potenziale minaccia per le istanze di database supportate.

> **Note**
>
> GuardDuty non gestisce la tua attività di accesso Database supportati o RDS e non ti rende disponibile l'attività di accesso RDS.

Configurazione della Protezione RDS per un account autonomo

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Protezione RDS.
3. La pagina Protezione RDS mostra lo stato attuale del tuo account. Puoi abilitare o disabilitare la funzionalità in qualsiasi momento selezionando Abilita o Disabilita. Conferma la selezione.

API/CLI

Esegui l'operazione API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il `name` dell'oggetto `features` su `RDS_LOGIN_EVENTS` e lo `status` su `ENABLED` o `DISABLED`.

È inoltre possibile abilitare o disabilitare la protezione RDS eseguendo il AWS CLI comando seguente. Assicurati di utilizzare il tuo *`ID rilevatore`* valido.

> **Note**
>
> Il codice di esempio seguente abilita la Protezione RDS. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

Configurazione della Protezione RDS in ambienti con più account

In un ambiente con più account, solo l'account GuardDuty amministratore delegato ha la possibilità di abilitare o disabilitare la funzionalità di protezione RDS per gli account dei membri della propria organizzazione. GuardDutyGli account membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce i propri account membro utilizzando AWS Organizations. Questo account GuardDuty amministratore delegato può scegliere di abilitare automaticamente il monitoraggio delle attività di accesso RDS per tutti i nuovi account

quando entrano a far parte dell'organizzazione. Per ulteriori informazioni sugli ambienti con più account, consulta Gestione di più account in Amazon. GuardDuty

Configurazione di RDS Protection per l'account amministratore delegato GuardDuty

Scegli il metodo di accesso preferito per configurare il monitoraggio delle attività di accesso RDS per l'account amministratore delegato. GuardDuty

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali dell'account di gestione.
2. Nel riquadro di navigazione, scegli Protezione RDS.
3. Nella pagina Protezione RDS, scegli Modifica.
4. Esegui una di queste operazioni:

   Utilizzando Abilita per tutti gli account

   - Scegli Abilita per tutti gli account. Ciò abiliterà il piano di protezione per tutti gli GuardDuty account attivi AWS dell'organizzazione, inclusi i nuovi account che entrano a far parte dell'organizzazione.
   - Selezionare Salva.

   Utilizzando Configura gli account manualmente

   - Per abilitare il piano di protezione solo per l'account GuardDuty amministratore delegato, scegli Configura gli account manualmente.
   - Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).
   - Selezionare Salva.

API/CLI

Esegui l'operazione API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il `name` dell'oggetto `features` su `RDS_LOGIN_EVENTS` e lo `status` su `ENABLED` o `DISABLED`.

È possibile abilitare o disabilitare la protezione RDS eseguendo il comando seguente AWS CLI . Assicurati di utilizzare l'ID *`rilevatore`* valido dell'account GuardDuty amministratore delegato.

> **Note**
>
> Il codice di esempio seguente abilita la Protezione RDS. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 555555555555 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

Abilitare automaticamente la Protezione RDS per tutti gli account membri

Scegli il metodo di accesso che preferisci per abilitare la funzionalità di Protezione RDS per tutti gli account membri, inclusi gli account membri esistenti e i nuovi account che entrano a far parte dell'organizzazione.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.
2. Esegui una di queste operazioni:

   Utilizzando la pagina Protezione RDS

   1. Nel riquadro di navigazione, scegli Protezione RDS.
   2. Scegli Abilita per tutti gli account. Questa operazione abilita automaticamente la Protezione RDS per gli account dell'organizzazione esistenti e per quelli nuovi.
   3. Selezionare Salva.

      > **Note**
      >
      > L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Utilizzando la pagina Account

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
3. Nella finestra Gestisci le preferenze di abilitazione automatica, scegli Abilita per tutti gli account in Monitoraggio delle attività di accesso RDS.
4. Selezionare Salva.

Se non puoi utilizzare l'opzione Abilita per tutti gli account, consulta Abilitare o disabilitare in modo selettivo la Protezione RDS per gli account membri.

API/CLI

- Per abilitare o disabilitare in modo selettivo la Protezione RDS per i tuoi account membri, richiama l'operazione API updateMemberDetectors utilizzando il tuo *ID rilevatore*.
- L'esempio seguente mostra come abilitare la Protezione RDS per un singolo account membro. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

  Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

  > **Note**
  >
  > Puoi anche trasmettere un elenco di ID account separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare la Protezione RDS per tutti gli account membri attivi esistenti

Scegli il metodo di accesso che preferisci per abilitare la Protezione RDS per tutti gli account membri attivi esistenti dell'organizzazione.

Console

Per configurare la Protezione RDS per tutti gli account membri attivi esistenti

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.
2. Nel riquadro di navigazione, scegli Protezione RDS.
3. Nella pagina Protezione RDS, puoi visualizzare lo stato attuale della configurazione. Nella sezione Account membri attivi, scegli Operazioni.
4. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
5. Scegli Conferma.

API/CLI

- Per abilitare o disabilitare in modo selettivo la Protezione RDS per i tuoi account membri, richiama l'operazione API updateMemberDetectors utilizzando il tuo *`ID rilevatore`*.
- L'esempio seguente mostra come abilitare la Protezione RDS per un singolo account membro. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

  Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

  > **Note**
  >
  > Puoi anche trasmettere un elenco di ID account separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare automaticamente la Protezione RDS per i nuovi account membri

Scegli il metodo di accesso che preferisci per abilitare l'attività di accesso RDS per i nuovi account che entrano a far parte dell'organizzazione.

Console

L'account GuardDuty amministratore delegato può abilitare nuovi account membro in un'organizzazione tramite la console, utilizzando la pagina Protezione RDS o Account.

Per abilitare automaticamente la Protezione RDS per i nuovi account membri

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.
2. Esegui una di queste operazioni:
   - Utilizzando la pagina Protezione RDS:
     1. Nel riquadro di navigazione, scegli Protezione RDS.
     2. Nella pagina Protezione RDS, scegli Modifica.
     3. Scegli Configura gli account manualmente.
     4. Seleziona Abilita automaticamente per i nuovi account membri. Questa fase garantisce l'abilitazione automatica della Protezione RDS per ogni nuovo account che entra a far parte dell'organizzazione. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa configurazione.
     5. Selezionare Salva.
   - Utilizzando la pagina Account:
     1. Dal riquadro di navigazione, selezionare Accounts (Account).
     2. Nella pagina Account, scegli le preferenze di Abilitazione automatica.
     3. Nella finestra Gestisci le preferenze di abilitazione automatica, seleziona Abilita per nuovi account in Monitoraggio delle attività di accesso RDS.

4. Selezionare Salva.

API/CLI

- Per abilitare o disabilitare in modo selettivo la Protezione RDS per i tuoi account membri, richiama l'operazione API UpdateOrganizationConfiguration utilizzando il tuo *ID rilevatore*.
- L'esempio seguente mostra come abilitare la Protezione RDS per un singolo account membro. Per disabilitarla, consulta Abilitare o disabilitare in modo selettivo la Protezione RDS per gli account membri. Se non desideri abilitarlo per tutti i nuovi account che entrano a far parte dell'organizzazione, imposta `autoEnable` su `NONE`.

  Per trovare l'`detectorId`account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

  > **Note**
  >
  > Puoi anche trasmettere un elenco di ID account separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare o disabilitare in modo selettivo la Protezione RDS per gli account membri

Scegli il metodo di accesso che preferisci per abilitare o disabilitare in modo selettivo l'attività di accesso RDS per gli account membri.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.
2. Dal riquadro di navigazione, selezionare Accounts (Account).

Nella pagina Account, consulta la colonna Attività di accesso RDS per visualizzare lo stato del tuo account membro.

3. Per abilitare o disabilitare in modo selettivo l'attività di accesso RDS

   Seleziona l'account per il quale desideri configurare la Protezione RDS. Puoi selezionare più account alla volta. Nel menu a discesa Modifica piani di protezione, scegli Attività di accesso RDS, quindi scegli l'opzione appropriata.

API/CLI

Per abilitare o disabilitare in modo selettivo la Protezione RDS per i tuoi account membri, richiama l'operazione API updateMemberDetectors utilizzando il tuo *`ID rilevatore`*.

L'esempio seguente mostra come abilitare la Protezione RDS per un singolo account membro. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

> **Note**
>
> Puoi anche trasmettere un elenco di ID account separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Funzionalità della Protezione RDS

Monitoraggio delle attività di accesso RDS

L'attività di accesso RDS rileva sia i tentativi di accesso riusciti che quelli falliti effettuati sul Database Amazon Aurora supportati nel tuo ambiente AWS . Per aiutarti a proteggere i tuoi database, GuardDuty RDS Protection monitora continuamente l'attività di accesso alla ricerca di tentativi di accesso potenzialmente sospetti. Ad esempio, un avversario potrebbe tentare un accesso di forza bruta a un database Amazon Aurora cercando di indovinarne la password.

Quando abiliti la funzionalità RDS Protection, inizia GuardDuty automaticamente a monitorare l'attività di accesso RDS per i tuoi database direttamente dal servizio Aurora. Se c'è un'indicazione di un comportamento di accesso anomalo, GuardDuty genera un risultato con dettagli sul database potenzialmente compromesso. Quando abiliti la Protezione RDS per la prima volta o hai un'istanza di database appena creata, è necessario un periodo di apprendimento per definire il comportamento normale. Per questo motivo, alle istanze di database appena abilitate o appena create potrebbero non essere associati esiti relativi a un accesso anomalo per un massimo di due settimane.

La funzionalità RDS Protection non richiede alcuna configurazione aggiuntiva; non influisce su nessuna delle configurazioni esistenti del database Amazon Aurora. GuardDuty non gestisce i database supportati o l'attività di accesso RDS né rende disponibile l'attività di accesso RDS.

Se scegli di abilitare automaticamente la funzionalità di protezione RDS per i nuovi account membro quando entrano a far parte dell'organizzazione, questa azione abilita GuardDuty automaticamente tali nuovi account membro. Per ulteriori informazioni sulla configurazione della funzionalità di monitoraggio delle attività di accesso RDS, consulta GuardDuty Protezione RDS.

GuardDuty Monitoraggio del runtime

Runtime Monitoring osserva e analizza gli eventi a livello di sistema operativo, di rete e di file per aiutarti a rilevare potenziali minacce in carichi di AWS lavoro specifici del tuo ambiente.

GuardDuty inizialmente ha rilasciato Runtime Monitoring per supportare solo le risorse Amazon Elastic Kubernetes Service (Amazon EKS). Tuttavia, ora puoi anche utilizzare la funzionalità Runtime Monitoring per rilevare le minacce per le tue risorse AWS Fargate Amazon Elastic Container Service (Amazon ECS) e Amazon Elastic Compute Cloud (Amazon EC2).

In questo documento e in altre sezioni relative al Runtime Monitoring, GuardDuty utilizza la terminologia del tipo di risorsa per fare riferimento alle risorse Amazon EKS, Fargate, Amazon ECS e Amazon EC2.

Runtime Monitoring utilizza un agente GuardDuty di sicurezza che aggiunge visibilità al comportamento di runtime, come l'accesso ai file, l'esecuzione dei processi, gli argomenti della riga di comando e le connessioni di rete. Per ogni tipo di risorsa che desideri monitorare per rilevare potenziali minacce, puoi gestire l'agente di sicurezza per quel tipo di risorsa specifico automaticamente o manualmente (ad eccezione di Fargate (solo Amazon ECS)). La gestione automatica del security agent significa che autorizzi l'installazione e l'aggiornamento del security agent GuardDuty per tuo conto. D'altra parte, quando gestisci manualmente il security agent per le tue risorse, sei responsabile dell'installazione e dell'aggiornamento del security agent, se necessario.

Grazie a questa funzionalità estesa, GuardDuty può aiutarvi a identificare e rispondere a potenziali minacce che possono colpire le applicazioni e i dati in esecuzione nei singoli carichi di lavoro e istanze. Ad esempio, una minaccia può iniziare potenzialmente compromettendo un singolo contenitore che esegue un'applicazione web vulnerabile. Questa applicazione Web potrebbe disporre delle autorizzazioni di accesso ai contenitori e ai carichi di lavoro sottostanti. In questo scenario, credenziali configurate in modo errato potrebbero potenzialmente portare a un accesso più ampio all'account e ai dati in esso archiviati.

Analizzando gli eventi di runtime dei singoli contenitori e carichi di lavoro, è GuardDuty possibile identificare la compromissione di un container e delle relative AWS credenziali in una fase iniziale e rilevare tentativi di aumentare i privilegi, le richieste API sospette e l'accesso malevolo ai dati nell'ambiente.

Indice

- Come funziona

- Come funziona la versione di prova gratuita di 30 giorni in Runtime Monitoring
- Prerequisiti per abilitare il monitoraggio del runtime
- Concetti chiave: approcci alla gestione degli agenti GuardDuty di sicurezza
- Abilitazione del monitoraggio del GuardDuty runtime
- Configurazione di EKS Runtime Monitoring (solo API)
- Migrazione da EKS Runtime Monitoring a Runtime Monitoring
- Valutazione della copertura in fase di esecuzione delle risorse
- Configurazione del monitoraggio della CPU e della memoria
- Tipi di eventi di runtime raccolti che utilizza GuardDuty
- Agente di hosting del repository Amazon ECR GuardDuty
- GuardDuty cronologia delle versioni degli agenti

Come funziona

Per utilizzare Runtime Monitoring, è necessario abilitare il Runtime Monitoring e quindi gestire il security agent. GuardDuty L'elenco seguente illustra questo processo in due fasi:

1. Abilita il monitoraggio del runtime per il tuo account in modo che GuardDuty possa accettare gli eventi di runtime che riceve dalle tue istanze Amazon EC2, dai cluster Amazon ECS e dai carichi di lavoro Amazon EKS.
2. Gestisci GuardDuty l'agente per le singole risorse di cui desideri monitorare il comportamento di runtime. In base al tipo di risorsa, è possibile scegliere di distribuire il GuardDuty security agent manualmente o consentendone la gestione GuardDuty per conto dell'utente, operazione denominata configurazione automatizzata dell'agente.

   GuardDuty utilizza i ruoli di identità dell'istanza che autenticano il security agent per ogni tipo di risorsa per inviare gli eventi di runtime associati all'endpoint VPC.

> **Note**
>
> GuardDuty non gestisce gli eventi di runtime per le tue istanze Amazon EC2, i cluster Amazon ECS o i cluster Amazon EKS, né li rende accessibili a te.

Quando gestisci l'agente di sicurezza (manualmente o tramite GuardDuty) in EKS Runtime Monitoring o Runtime Monitoring for EC2 e GuardDuty viene attualmente distribuito su un'istanza Amazon EC2 e riceve i dati Tipi di eventi di runtime raccolti da questa istanza, non GuardDuty ti verrà addebitato alcun costo per Account AWS l'analisi dei log di flusso VPC da questa istanza Amazon EC2. Questo aiuta a GuardDuty evitare il doppio dei costi di utilizzo dell'account.

I seguenti argomenti spiegano come l'attivazione del Runtime Monitoring e la gestione del GuardDuty Security Agent funzionino in modo diverso per ogni tipo di risorsa.

Indice

- Come funziona il monitoraggio del runtime con le istanze Amazon EC2
- Come funziona il monitoraggio del runtime con Fargate (solo Amazon ECS)
- Come funziona il monitoraggio del runtime con i cluster Amazon EKS
- Dopo la configurazione del monitoraggio del runtime

Come funziona il monitoraggio del runtime con le istanze Amazon EC2

Le tue istanze Amazon EC2 possono eseguire diversi tipi di applicazioni e carichi di lavoro nel tuo ambiente. AWS Quando abiliti il monitoraggio del runtime e gestisci l'agente GuardDuty di sicurezza, ti GuardDuty aiuta a rilevare le minacce nelle istanze Amazon EC2 esistenti e in quelle potenzialmente nuove. Questa funzionalità supporta anche le istanze Amazon EC2 gestite da Amazon ECS.

L'abilitazione del monitoraggio del runtime consente GuardDuty di utilizzare gli eventi di runtime dei processi attualmente in esecuzione e dei nuovi processi all'interno delle istanze Amazon EC2. GuardDuty richiede un agente di sicurezza a cui inviare gli eventi di runtime dall'istanza EC2 a. GuardDuty

Per le istanze Amazon EC2, il GuardDuty security agent opera a livello di istanza. Puoi decidere se monitorare tutte le istanze Amazon EC2 o solo alcune istanze Amazon EC2 nel tuo account. Se desideri gestire istanze selettive, l'agente di sicurezza è necessario solo per queste istanze.

GuardDuty può anche utilizzare eventi di runtime da nuove attività e attività esistenti in esecuzione in istanze Amazon EC2 all'interno di cluster Amazon ECS.

Per installare l'agente GuardDuty di sicurezza, Runtime Monitoring offre le seguenti due opzioni:

- Utilizza la configurazione automatica degli agenti (scelta consigliata), oppure

- Gestisci manualmente l'agente di sicurezza

Utilizza la configurazione automatica degli agenti tramite GuardDuty (consigliato)

Utilizza la configurazione automatizzata dell'agente che consente GuardDuty di installare l'agente di sicurezza sulle tue istanze Amazon EC2 per tuo conto. GuardDuty gestisce anche gli aggiornamenti del security agent.

Per impostazione predefinita, GuardDuty installa il security agent su tutte le istanze del tuo account. Se desideri GuardDuty installare e gestire il security agent solo per istanze EC2 selezionate, aggiungi tag di inclusione o esclusione alle tue istanze EC2, se necessario.

A volte, potresti non voler monitorare gli eventi di runtime per tutte le istanze Amazon EC2 che appartengono al tuo account. Nei casi in cui desideri monitorare gli eventi di runtime per un numero limitato di istanze, aggiungi un tag di inclusione come`GuardDutyManaged`: `true` a queste istanze selezionate. A partire dalla disponibilità della configurazione automatizzata degli agenti per Amazon EC2, se l'istanza EC2 ha un tag di inclusione (`GuardDutyManaged`:`true`), GuardDuty rispetterà il tag e gestirà il security agent per le istanze selezionate anche quando non abiliti esplicitamente la configurazione automatica dell'agente.

D'altra parte, se esiste un numero limitato di istanze EC2 per le quali non desideri monitorare gli eventi di runtime, aggiungi un tag di esclusione (:) `GuardDutyManaged` a queste istanze selezionate. `false` GuardDuty rispetterà il tag di esclusione non installando né gestendo il security agent per queste risorse EC2.

Impatto

Quando utilizzi la configurazione automatizzata degli agenti in un'organizzazione Account AWS o in un'organizzazione, autorizzi GuardDuty a eseguire le seguenti operazioni per tuo conto:

- GuardDuty crea un'associazione SSM per tutte le istanze Amazon EC2 gestite da SSM e visualizzate in Fleet Manager nella console https://console.aws.amazon.com/systems-manager/.
- Utilizzo dei tag di inclusione con la configurazione automatica dell'agente disabilitata: dopo aver abilitato il Runtime Monitoring, quando non abiliti la configurazione automatica dell'agente ma aggiungi il tag di inclusione alla tua istanza Amazon EC2, significa che stai autorizzando GuardDuty a gestire il security agent per tuo conto. L'associazione SSM installerà quindi l'agente di sicurezza in ogni istanza che presenta il tag di inclusione (:)`GuardDutyManaged`. `true`
- Se abiliti la configurazione automatica dell'agente, l'associazione SSM installerà quindi il security agent in tutte le istanze EC2 che appartengono al tuo account.

- Utilizzo dei tag di esclusione con la configurazione automatica degli agenti: prima di abilitare la configurazione automatica degli agenti, quando aggiungi un tag di esclusione alla tua istanza Amazon EC2, significa che stai GuardDuty autorizzando a impedire l'installazione e la gestione del security agent per l'istanza selezionata.

  Ora, quando abiliti la configurazione automatizzata dell'agente, l'associazione SSM installerà e gestirà il security agent in tutte le istanze EC2 ad eccezione di quelle contrassegnate con il tag di esclusione.
- GuardDuty crea endpoint VPC in tutti i VPC, compresi i VPC condivisi, purché in quel VPC sia presente almeno un'istanza Linux EC2 che non si trovi nello stato di terminazione o di chiusura dell'istanza. Per informazioni sui diversi stati delle istanze, consulta il ciclo di vita delle istanze nella Guida per l'utente di Amazon EC2 per le istanze Linux.

  GuardDuty supporta anche. Utilizzo di VPC condiviso con agenti di sicurezza automatizzati Dopo aver considerato tutti i prerequisiti per l'organizzazione Account AWS, GuardDuty utilizzerà il VPC condiviso per ricevere eventi di runtime.

  > **Note**
  >
  > Non sono previsti costi aggiuntivi per l'utilizzo degli endpoint VPC creati. GuardDuty

Gestisci manualmente l'agente di sicurezza

Esistono due modi per gestire manualmente l'agente di sicurezza per Amazon EC2:

- Utilizza i documenti GuardDuty gestiti AWS Systems Manager per installare l'agente di sicurezza sulle tue istanze Amazon EC2 che sono già gestite tramite SSM.

  Ogni volta che avvii una nuova istanza Amazon EC2, assicurati che sia abilitata SSM.
- Usa gli script RPM Package Manager (RPM) per installare il security agent sulle tue istanze Amazon EC2, indipendentemente dal fatto che siano gestite tramite SSM o meno.

Approfondimenti

Per iniziare a utilizzare la configurazione di Runtime Monitoring per monitorare le istanze Amazon EC2, consulta. Prerequisiti per il supporto delle istanze Amazon EC2

Come funziona il monitoraggio del runtime con Fargate (solo Amazon ECS)

Quando abiliti il monitoraggio del runtime, GuardDuty diventa pronto a consumare gli eventi di runtime di un'attività. Queste attività vengono eseguite all'interno dei cluster Amazon ECS, che a loro volta vengono eseguiti sulle AWS Fargate (Fargate) istanze. GuardDuty Per ricevere questi eventi di runtime, devi utilizzare il security agent dedicato e completamente gestito.

Attualmente, Runtime Monitoring non supporta le attività avviate da and. AWS Batch AWS CodePipeline

Attualmente, Runtime Monitoring supporta la gestione dell'agente di sicurezza per i cluster Amazon ECS (AWS Fargate) solo tramite. GuardDuty Non è disponibile alcun supporto per la gestione manuale del security agent sui cluster Amazon ECS.

Puoi consentire la gestione del GuardDuty security agent GuardDuty per tuo conto, utilizzando la configurazione automatizzata dell'agente per un AWS account o un'organizzazione. GuardDuty inizierà a distribuire il security agent nelle nuove attività di Fargate che vengono lanciate nei cluster Amazon ECS. L'elenco seguente specifica cosa aspettarsi quando si abilita il security agent. GuardDuty

Impatto dell'attivazione del GuardDuty Security Agent

GuardDuty crea un endpoint di cloud privato virtuale (VPC)

Quando si distribuisce il GuardDuty security agent, GuardDuty verrà creato un endpoint VPC attraverso il quale il security agent consegna gli eventi di runtime. GuardDuty

GuardDuty aggiunge un contenitore sidecar

Per una nuova attività o servizio Fargate che inizia a funzionare, un GuardDuty container (sidecar) si collega a ciascun contenitore all'interno dell'attività Amazon ECS Fargate. L'agente di GuardDuty sicurezza viene eseguito all'interno del contenitore collegato. GuardDuty Questo aiuta GuardDuty a raccogliere gli eventi di runtime di ogni contenitore in esecuzione nell'ambito di queste attività.

Quando si avvia un'attività Fargate, se il GuardDuty contenitore (sidecar) non è in grado di avviarsi in uno stato integro, il Runtime Monitoring è progettato per non impedire l'esecuzione delle attività.

Per impostazione predefinita, un'attività Fargate è immutabile. GuardDuty non distribuirà il sidecar quando un'attività è già in esecuzione. Se desideri monitorare un contenitore in un'attività già in esecuzione, puoi interrompere l'attività e riavviarla.

Come funziona il monitoraggio del runtime con i cluster Amazon EKS

Runtime Monitoring utilizza un componente aggiuntivo EKS `aws-guardduty-agent`, chiamato anche agente di GuardDuty sicurezza. Dopo che l'agente GuardDuty di sicurezza è stato distribuito sui cluster EKS, GuardDuty è in grado di ricevere eventi di runtime per questi cluster EKS.

Puoi monitorare gli eventi di runtime dei tuoi cluster Amazon EKS a livello di account o di cluster. Puoi gestire l'agente GuardDuty di sicurezza solo per i cluster Amazon EKS che desideri monitorare per il rilevamento delle minacce. Puoi gestire l'agente GuardDuty di sicurezza manualmente o consentendone la gestione GuardDuty per tuo conto, utilizzando la configurazione automatizzata dell'agente.

Quando utilizzi l'approccio di configurazione automatizzata dell'agente GuardDuty per consentire di gestire l'implementazione del security agent per tuo conto, questo creerà automaticamente un endpoint Amazon Virtual Private Cloud (Amazon VPC). Il security agent fornisce gli eventi di runtime GuardDuty utilizzando questo endpoint Amazon VPC.

Attualmente GuardDuty supporta i cluster Amazon EKS in esecuzione su istanze Amazon EC2. GuardDuty non supporta i cluster Amazon EKS in esecuzione su AWS Fargate.

Dopo la configurazione del monitoraggio del runtime

Valuta la copertura del runtime

Dopo aver abilitato il Runtime Monitoring e distribuito il GuardDuty security agent, ti consigliamo di valutare continuamente lo stato di copertura della risorsa in cui hai distribuito il security agent. Lo stato della copertura potrebbe essere Inintegro o Non integro. Uno stato di copertura integro indica che GuardDuty sta ricevendo gli eventi di runtime dalla risorsa corrispondente quando è in corso un'attività a livello di sistema operativo.

Quando lo stato di copertura diventa Inattivo per la risorsa, GuardDuty è in grado di ricevere gli eventi di runtime e analizzarli per il rilevamento delle minacce. Quando GuardDuty rileva una potenziale minaccia alla sicurezza nelle attività o nelle applicazioni in esecuzione nei carichi di lavoro e nelle istanze del container, GuardDuty genera uno o più tipi di risultati di Runtime Monitoring.

[1] Puoi anche configurare Amazon EventBridge (EventBridge) per ricevere una notifica quando lo stato della copertura cambia da Insalutare a Healthy e altro.

Per ulteriori informazioni, consulta Valutazione della copertura in fase di esecuzione delle risorse.

GuardDuty rileva potenziali minacce

Quando GuardDuty inizia a ricevere gli eventi di runtime della risorsa, inizia ad analizzarli. Quando GuardDuty rileva una potenziale minaccia alla sicurezza in una delle tue istanze Amazon EC2, nei cluster Amazon ECS o nei cluster Amazon EKS, ne genera una o più. Tipi di risultati del monitoraggio del runtime Puoi accedere ai dettagli dei risultati per visualizzare i dettagli delle risorse interessate.

Come funziona la versione di prova gratuita di 30 giorni in Runtime Monitoring

Il periodo di prova gratuito di 30 giorni funziona in modo diverso per i nuovi GuardDuty account e per gli account esistenti che hanno già abilitato EKS Runtime Monitoring prima che la funzionalità di Runtime Monitoring fosse estesa alle istanze Amazon EC2 e AWS Fargate (solo Amazon ECS).

Sto usando il periodo di GuardDuty prova o non ho mai abilitato EKS Runtime Monitoring

L'elenco seguente spiega come funziona il periodo di prova gratuito di 30 giorni se utilizzi il periodo di prova di GuardDuty 30 giorni o non hai mai abilitato EKS Runtime Monitoring:

- Quando si abilita GuardDuty per la prima volta, il Runtime Monitoring e EKS Runtime Monitoring non saranno abilitati per impostazione predefinita.

  Quando abiliti il Runtime Monitoring per il tuo account o la tua organizzazione, assicurati di configurare anche il GuardDuty security agent per la risorsa che desideri monitorare per il rilevamento delle minacce. Ad esempio, se desideri utilizzare Runtime Monitoring per le tue istanze Amazon EC2, dopo aver abilitato il Runtime Monitoring, devi configurare anche l'agente di sicurezza per Amazon EC2. Puoi scegliere di farlo manualmente o automaticamente tramite. GuardDuty
- Il piano di protezione del Runtime Monitoring è abilitato a livello di account. Il periodo di prova gratuito di 30 giorni funziona a livello di risorse. Dopo la distribuzione del GuardDuty Security Agent

su un tipo di risorsa specifico, la prova gratuita di 30 giorni inizia quando GuardDuty riceve il primo evento di runtime associato a questo tipo di risorsa. Ad esempio, hai distribuito l' GuardDuty agente a livello di risorsa (per l'istanza Amazon EC2, il cluster Amazon ECS e il cluster Amazon EKS). Quando GuardDuty riceve il primo evento di runtime per un'istanza Amazon EC2, la prova gratuita di 30 giorni inizierà solo per Amazon EC2.

- Quando desideri abilitare solo EKS Runtime Monitoring — Quando lo abiliti GuardDuty per la prima volta, EKS Runtime Monitoring non è abilitato per impostazione predefinita (dopo il rilascio di Runtime Monitoring). Dovrai abilitare EKS Runtime Monitoring. Per utilizzarlo in modo ottimale, assicuratevi di gestire il GuardDuty security agent manualmente o di abilitare la configurazione automatizzata dell'agente in modo che GuardDuty gestisca l'agente per vostro conto. Il periodo di prova gratuito di 30 giorni per EKS Runtime Monitoring inizia quando GuardDuty riceve il primo evento di runtime per la risorsa Amazon EKS.

Ho abilitato EKS Runtime Monitoring prima del lancio di Runtime Monitoring

- Per un GuardDuty account esistente che ha il piano di protezione EKS Runtime Monitoring abilitato e utilizza l'esperienza della GuardDuty console per utilizzare questo piano di protezione: con l'annuncio di Runtime Monitoring, l'esperienza della console EKS Runtime Monitoring è stata ora consolidata nel Runtime Monitoring. La configurazione esistente per EKS Runtime Monitoring rimane la stessa. È possibile continuare a utilizzare il supporto API/CLI per eseguire operazioni associate a EKS Runtime Monitoring.
- Per utilizzare EKS Runtime Monitoring come parte del Runtime Monitoring, è necessario configurare il Runtime Monitoring per l'account o l'organizzazione. Per mantenere la stessa configurazione per Runtime Monitoring, vediMigrazione da EKS Runtime Monitoring a Runtime Monitoring. Tuttavia, ciò non influirà sulla prova gratuita di 30 giorni per la risorsa Amazon EKS.
- Il piano di protezione del Runtime Monitoring è abilitato a livello di account. Dopo la distribuzione del GuardDuty security agent su uno dei tipi di risorse specificati (istanza Amazon EC2 e cluster Amazon ECS), la prova gratuita di 30 giorni inizia GuardDuty quando riceve il primo evento di runtime associato alla risorsa. È disponibile una prova gratuita di 30 giorni associata a ciascun tipo di risorsa.

  Ad esempio, dopo aver abilitato il Runtime Monitoring, scegli di distribuire l' GuardDuty agente solo su un'istanza Amazon EC2, la prova gratuita di 30 giorni per questa risorsa inizierà solo GuardDuty quando riceverà il primo evento di runtime per un'istanza Amazon EC2. Successivamente, quando distribuirai l' GuardDuty agente per Fargate (solo Amazon ECS), la prova gratuita di 30 giorni per questa risorsa inizierà solo GuardDuty quando riceverà il primo evento di runtime per il cluster

Amazon ECS. Considerando che hai già abilitato EKS Runtime Monitoring per il tuo account, GuardDuty non ripristina la prova gratuita di 30 giorni per una risorsa Amazon EKS.

Prerequisiti per abilitare il monitoraggio del runtime

Per abilitare il Runtime Monitoring e gestire il GuardDuty security agent, è necessario soddisfare i prerequisiti per ogni tipo di risorsa che si desidera monitorare per il rilevamento delle minacce.

Indice

- Prerequisiti per il supporto delle istanze Amazon EC2
- Prerequisiti per il AWS Fargate supporto (solo Amazon ECS)
- Prerequisiti per il supporto dei cluster Amazon EKS

Prerequisiti per il supporto delle istanze Amazon EC2

Prerequisito generale

Le istanze Amazon EC2 per le quali desideri GuardDuty monitorare gli eventi di runtime devono essere gestite tramite SSM. Questo indipendentemente dal fatto che tu lo utilizzi GuardDuty per gestire il security agent automaticamente o manualmente (tranne). Metodo 2: utilizzando gli script di installazione RPM

Per gestire le istanze Amazon EC2 con AWS Systems Manager, consulta Configurazione delle istanze di Systems Manager per Amazon EC2 nella Guida per l'utente.AWS Systems Manager

Convalida dei requisiti relativi all'architettura

L'architettura della distribuzione del sistema operativo potrebbe influire sul comportamento del GuardDuty security agent. È necessario soddisfare i seguenti requisiti prima di utilizzare Runtime Monitoring per le istanze Amazon EC2:

- Attualmente, il supporto per il monitoraggio del runtime per Amazon EC2 è disponibile solo per le versioni Linux. Sebbene il supporto per Ubuntu non sia disponibile al momento, lo sarà nelle prossime future. Per ricevere notifiche sugli aggiornamenti di questa pagina, iscriviti al feed RSS.

  La tabella seguente mostra la distribuzione del sistema operativo che è stata verificata per supportare l'agente GuardDuty di sicurezza per le istanze Amazon EC2.

Distribuzione del sistema operativo	Versione del kernel	Supporto del kernel	Architettura della CPU	
			x64 (AMD64)	Graviton (ARM64)
AL2 e AL2023	5.4, 5.10, 5.15, 6.1	eBPF, Tracepoints, Kprobe	Supportato	Supportato

- Requisiti aggiuntivi: solo se disponi di Amazon ECS/Amazon EC2

  Per Amazon ECS/Amazon EC2, ti consigliamo di utilizzare le AMI più recenti ottimizzate per Amazon ECS (datate 29 settembre 2023 o successive) o di utilizzare la versione dell'agente Amazon ECS v1.77.0.

Quando si utilizza la configurazione automatica degli agenti

Per Utilizza la configurazione automatica degli agenti (scelta consigliata) farlo, Account AWS è necessario soddisfare i seguenti prerequisiti:

- Quando utilizzi tag di inclusione con configurazione automatica degli agenti, per GuardDuty creare un'associazione SSM per una nuova istanza, assicurati che la nuova istanza sia gestita tramite SSM e venga visualizzata in Fleet Manager nella console https://console.aws.amazon.com/systems-manager/.
- Quando si utilizzano tag di esclusione con configurazione automatica degli agenti:
  - Aggiungi il `false` tag`GuardDutyManaged`: prima di configurare l'agente GuardDuty automatico per il tuo account.

    Assicurati di aggiungere il tag di esclusione alle istanze Amazon EC2 prima di avviarle. Quando abiliti la configurazione automatizzata degli agenti per Amazon EC2, qualsiasi istanza EC2 che viene avviata senza un tag di esclusione sarà coperta dalla configurazione automatizzata dell'agente. GuardDuty
  - Affinché i tag di esclusione funzionino, aggiorna la configurazione dell'istanza in modo che il documento di identità dell'istanza sia disponibile nel servizio di metadati dell'istanza (IMDS). La procedura per eseguire questo passaggio è già inclusa nel tuo accountAbilitazione del monitoraggio del runtime.

Limite di CPU e memoria per GuardDuty l'agente

Limite della CPU

Il limite massimo di CPU per il GuardDuty security agent associato alle istanze Amazon EC2 è pari al 10% dei core vCPU totali. Ad esempio, se l'istanza EC2 ha 4 core vCPU, il security agent può utilizzare al massimo il 40 percento del 400 percento totale disponibile.

Memory limit (Limite memoria)

Dalla memoria associata all'istanza Amazon EC2, c'è una memoria limitata che il GuardDuty security agent può utilizzare.

La tabella seguente mostra il limite di memoria.

Memoria dell'istanza Amazon EC2	Memoria massima per l'agente GuardDuty
Meno di 8 GB	128 MB
Meno di 32 GB	256 MB
Maggiore o uguale a 32 GB	1 GB

Approfondimenti

Il passaggio successivo consiste nella configurazione del Runtime Monitoring e nella gestione del security agent (automaticamente o manualmente). Per ulteriori informazioni, consulta Abilitazione del monitoraggio del runtime.

Prerequisiti per il AWS Fargate supporto (solo Amazon ECS)

Convalida dei requisiti relativi all'architettura

La piattaforma utilizzata può influire sul modo GuardDuty in cui il GuardDuty Security Agent supporta la ricezione degli eventi di runtime dai cluster Amazon ECS. Devi confermare di utilizzare una delle piattaforme verificate.

Considerazioni iniziali:

La AWS Fargate (Fargate) piattaforma per i tuoi cluster Amazon ECS deve essere Linux. La versione della piattaforma corrispondente deve essere almeno`1.4.0`, o. `LATEST` Per ulteriori

informazioni sulle versioni della piattaforma, consulta le versioni della piattaforma Linux nella Amazon Elastic Container Service Developer Guide.

Le versioni della piattaforma Windows non sono ancora supportate.

Piattaforme verificate

La distribuzione del sistema operativo e l'architettura della CPU influiscono sul supporto fornito dal GuardDuty security agent. La tabella seguente mostra la configurazione verificata per la distribuzione del GuardDuty security agent e la configurazione del Runtime Monitoring.

Distribuzione del sistema operativo	Supporto del kernel	Architettura della CPU	
		x64 (AMD64)	Graviton (ARM64)
Linux	eBPF, Tracepoints, Kprobe	Supported	Supported

Fornisci le autorizzazioni ECR e i dettagli della sottorete

Prima di abilitare Runtime Monitoring, è necessario fornire i seguenti dettagli:

Fornisci un ruolo di esecuzione dell'attività con autorizzazioni

Il ruolo di esecuzione delle attività richiede che tu disponga di determinate autorizzazioni Amazon Elastic Container Registry (Amazon ECR). Puoi utilizzare la politica gestita di TaskExecutionRolePolicyAmazonECS o aggiungere le seguenti autorizzazioni alla tua politica: `TaskExecutionRole`

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

Per limitare ulteriormente le autorizzazioni di Amazon ECR, puoi aggiungere l'URI del repository Amazon ECR che ospita l'agente di GuardDuty sicurezza per (solo AWS Fargate Amazon ECS).

Per ulteriori informazioni, consulta Repository per GuardDuty agente su AWS Fargate (solo Amazon ECS).

Fornisci i dettagli della sottorete nella definizione dell'attività

Puoi fornire le sottoreti pubbliche come input nella definizione dell'attività o creare un endpoint VPC Amazon ECR.

- Utilizzo dell'opzione di definizione delle attività: l'esecuzione delle UpdateServiceAPI CreateServiceand nell'Amazon Elastic Container Service API Reference richiede il trasferimento delle informazioni sulla sottorete. Per ulteriori informazioni, consulta le definizioni delle attività di Amazon ECS nella Amazon Elastic Container Service Developer Guide.
- Utilizzo dell'opzione endpoint Amazon ECR VPC — Fornisci un percorso di rete ad Amazon ECR - Assicurati che l'URI del repository Amazon ECR che ospita GuardDuty il security agent sia accessibile dalla rete. Se le attività Fargate verranno eseguite in una sottorete privata, Fargate avrà bisogno del percorso di rete per scaricare il contenitore. GuardDuty

  Per informazioni su come abilitare Fargate a scaricare il GuardDuty contenitore, consulta Using Amazon ECR with Amazon ECS nella Amazon Elastic Container Service Developer Guide.

Limiti di CPU e di memoria

Nella definizione dell'attività Fargate, è necessario specificare il valore della CPU e della memoria a livello di attività. La tabella seguente mostra le combinazioni valide di valori di CPU e memoria a livello di task e il limite massimo di memoria del GuardDuty Security Agent corrispondente per il contenitore. GuardDuty

Valore CPU	Valore memoria	GuardDuty limite massimo di memoria dell'agente
256 (0,25 vCPU)	512 MiB, 1 GB, 2 GB	128 MB
512 (0,5 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)	Tra 4 GB e 16 GB in incrementi di 1 GB	

Valore CPU	Valore memoria	GuardDuty limite massimo di memoria dell'agente
4096 (4 vCPU)	Tra 8 GB e 20 GB con incrementi di 1 GB	256 MB
8192 (8 vCPU)	Tra 16 GB e 28 GB con incrementi di 4 GB	
	Tra 32 GB e 60 GB con incrementi di 4 GB	512 MB
16384 (16 vCPU)	Tra 32 GB e 120 GB in incrementi di 8 GB	1 GB

Dopo aver abilitato il Runtime Monitoring e verificato che lo stato di copertura del cluster sia integro, puoi configurare e visualizzare le metriche di Container Insight. Per ulteriori informazioni, consulta Configurazione del monitoraggio sul cluster Amazon ECS.

Il passaggio successivo consiste nella configurazione del Runtime Monitoring e nella gestione del security agent. Per ulteriori informazioni, consulta Abilitazione del monitoraggio del runtime.

Prerequisiti per il supporto dei cluster Amazon EKS

Convalida dei requisiti relativi all'architettura

La piattaforma utilizzata può influire sul modo GuardDuty in cui GuardDuty Security Agent supporta la ricezione degli eventi di runtime dai cluster EKS. Devi confermare di utilizzare una delle piattaforme verificate. Se gestisci l' GuardDuty agente manualmente, assicurati che la versione di Kubernetes supporti la versione dell' GuardDuty agente attualmente in uso.

Piattaforme verificate

La distribuzione del sistema operativo, la versione del kernel e l'architettura della CPU influiscono sul supporto fornito dal security agent. GuardDuty La tabella seguente mostra la configurazione verificata per l'implementazione del GuardDuty security agent e la configurazione di EKS Runtime Monitoring.

Versione del kernel	Supporto del kernel	Architettura della CPU

Distribuzione del sistema operativo			x64 (AMD64)	Graviton (ARM64) (Graviton2 e versioni successive) 1	Versione di Kubernetes supportata
Ubuntu AL2	5.4, 5.10, 5.15, 6.1	Tracepoints eBF, Kprobe	Supportato	Supportato	v1.21 - v1.29
Bottlerocket					v1.23 - v1.29

1. Il monitoraggio del runtime per i cluster Amazon EKS non supporta le istanze Graviton di prima generazione come i tipi di istanze A1.

Versioni di Kubernetes supportate dal security agent GuardDuty

La tabella seguente mostra le versioni di Kubernetes per i cluster EKS supportate dal security agent. GuardDuty

Versione di Kubernetes	Versione dell'agente di GuardDuty sicurezza aggiuntivo Amazon EKS							
	v1.5.0	v1.4.1	v1.4.0	v1.3.1	v1.3.0	v1.2.0	v1.1.0	v1.0.0
1,29	Supportato	Supportato	Supportato	Non supportato	Non supportato	Non supportato	Non supportato	Non supportato
1,28				Supportato	Supportato			
1,27						Supportato		
1,26							Supportato	

1,25	Supportato
1,24	
1,23	
1,22	
1,21	

Alcune versioni del GuardDuty Security Agent raggiungeranno la fine del supporto standard. Per informazioni sulle versioni di rilascio degli agenti, vedereGuardDuty agente di sicurezza per cluster Amazon EKS.

Limiti di CPU e di memoria

La tabella seguente mostra i limiti di CPU e memoria per il componente aggiuntivo Amazon EKS per GuardDuty (`aws-guardduty-agent`).

Parametro	Limite minimo	Limite massimo
CPU	200 m	1000 m
Memoria	256 Mi	1024 Mi

Quando utilizzi il componente aggiuntivo Amazon EKS versione 1.5.0 o successiva, GuardDuty offre la possibilità di configurare lo schema del componente aggiuntivo per i valori di CPU e memoria. Per informazioni sull'intervallo configurabile, consulta. Parametri e valori configurabili

Dopo aver abilitato il monitoraggio del runtime EKS e valutato lo stato di copertura dei cluster EKS, puoi configurare e visualizzare i parametri di Container Insights. Per ulteriori informazioni, consulta Configurazione del monitoraggio della CPU e della memoria.

Concetti chiave: approcci alla gestione degli agenti GuardDuty di sicurezza

Considera i concetti chiave che ti aiuteranno a gestire l'agente di sicurezza sui tuoi cluster Amazon EKS e Amazon ECS.

Indice

- Risorsa Fargate (solo Amazon ECS) - Approcci alla gestione degli agenti di sicurezza GuardDuty
- Cluster Amazon EKS: approcci alla gestione degli agenti GuardDuty di sicurezza

Risorsa Fargate (solo Amazon ECS) - Approcci alla gestione degli agenti di sicurezza GuardDuty

Runtime Monitoring ti offre la possibilità di rilevare potenziali minacce alla sicurezza su tutti i cluster Amazon ECS (a livello di account) o sui cluster selettivi (a livello di cluster) del tuo account. Quando abiliti la configurazione automatizzata degli agenti per ogni attività di Amazon ECS Fargate che verrà eseguita GuardDuty , aggiungerà un contenitore secondario per ogni carico di lavoro del container all'interno di tale attività. L'agente GuardDuty di sicurezza viene distribuito in questo contenitore secondario. In questo modo si GuardDuty ottiene visibilità sul comportamento di runtime dei contenitori all'interno delle attività di Amazon ECS.

Attualmente, Runtime Monitoring supporta la gestione dell'agente di sicurezza per i cluster Amazon ECS (AWS Fargate) solo tramite. GuardDuty Non è disponibile alcun supporto per la gestione manuale del security agent sui cluster Amazon ECS.

Prima di configurare i tuoi account, valuta come desideri gestire l'agente di GuardDuty sicurezza e potenzialmente monitora il comportamento di runtime dei contenitori che appartengono alle attività di Amazon ECS. Considera i seguenti approcci.

Argomenti

- Gestisci l'agente GuardDuty di sicurezza per tutti i cluster Amazon ECS
- Gestisci l'agente di GuardDuty sicurezza per la maggior parte dei cluster Amazon ECS ma escludi alcuni cluster Amazon ECS
- Gestisci l'agente GuardDuty di sicurezza per cluster Amazon ECS selettivi

Gestisci l'agente GuardDuty di sicurezza per tutti i cluster Amazon ECS

Questo approccio ti aiuterà a rilevare potenziali minacce alla sicurezza a livello di account. Utilizza questo approccio quando desideri rilevare potenziali minacce GuardDuty alla sicurezza per tutti i cluster Amazon ECS che appartengono al tuo account.

Gestisci l'agente di GuardDuty sicurezza per la maggior parte dei cluster Amazon ECS ma escludi alcuni cluster Amazon ECS

Utilizza questo approccio quando desideri rilevare potenziali minacce GuardDuty alla sicurezza per la maggior parte dei cluster Amazon ECS nel tuo AWS ambiente ma escluderne alcuni. Questo approccio ti aiuta a monitorare il comportamento di runtime dei container all'interno delle tue attività Amazon ECS a livello di cluster. Ad esempio, il numero di cluster Amazon ECS che appartengono al tuo account è 1000. Tuttavia, desideri monitorare solo 930 cluster Amazon ECS.

Questo approccio richiede l'aggiunta di un GuardDuty tag predefinito ai cluster Amazon ECS che non desideri monitorare. Per ulteriori informazioni, consulta Gestione dell'agente di sicurezza automatizzato per Fargate (solo Amazon ECS).

Gestisci l'agente GuardDuty di sicurezza per cluster Amazon ECS selettivi

Utilizza questo approccio quando desideri GuardDuty rilevare potenziali minacce alla sicurezza per alcuni cluster Amazon ECS. Questo approccio ti aiuta a monitorare il comportamento di runtime dei container all'interno delle tue attività Amazon ECS a livello di cluster. Ad esempio, il numero di cluster Amazon ECS che appartengono al tuo account è 1000. Tuttavia, desideri monitorare solo 230 cluster.

Questo approccio richiede l'aggiunta di un GuardDuty tag predefinito ai cluster Amazon ECS che desideri monitorare. Per ulteriori informazioni, consulta Gestione dell'agente di sicurezza automatizzato per Fargate (solo Amazon ECS).

Cluster Amazon EKS: approcci alla gestione degli agenti GuardDuty di sicurezza

GuardDuty Per utilizzare gli eventi di runtime dei cluster EKS a livello di account o di cluster, è necessario gestire il GuardDuty security agent per i cluster corrispondenti.

Approcci per gestire l'agente di sicurezza GuardDuty

Prima del 13 settembre 2023, era possibile GuardDuty configurare la gestione del security agent a livello di account. Questo comportamento indicava che, per impostazione predefinita, GuardDuty gestirà il security agent su tutti i cluster EKS che appartengono a un Account AWS. Ora GuardDuty fornisce una funzionalità granulare per aiutarvi a scegliere i cluster EKS in cui desiderate gestire l'agente GuardDuty di sicurezza.

Se scegli Gestisci l'agente GuardDuty di sicurezza manualmente, puoi comunque selezionare i cluster EKS che desideri monitorare. Tuttavia, per gestire l'agente manualmente, è necessario creare un endpoint Amazon VPC per Account AWS .

> **Note**
>
> Indipendentemente dall'approccio utilizzato per gestire l'agente di GuardDuty sicurezza, EKS Runtime Monitoring è sempre abilitato a livello di account.

Argomenti

- Gestisci l'agente di sicurezza tramite GuardDuty
- Gestisci l'agente GuardDuty di sicurezza manualmente

Gestisci l'agente di sicurezza tramite GuardDuty

GuardDuty implementa e gestisce il security agent per tuo conto. Puoi monitorare i cluster EKS nel tuo account in qualsiasi momento utilizzando uno degli approcci seguenti.

Argomenti

- Monitorare tutti i cluster EKS
- Monitorare tutti i cluster EKS ed escludere cluster EKS selettivi
- Monitorare cluster EKS selettivi

Monitorare tutti i cluster EKS

- Quando utilizzare questo approccio: utilizza questo approccio quando desideri GuardDuty implementare e gestire il security agent per tutti i cluster EKS del tuo account. Per impostazione predefinita, GuardDuty implementerà il security agent anche su un cluster EKS potenzialmente nuovo creato nel tuo account.
- Impatto dell'utilizzo di questo approccio:
  - GuardDuty crea un endpoint Amazon Virtual Private Cloud (Amazon VPC) attraverso il quale il GuardDuty security agent consegna gli eventi di runtime. GuardDuty Non sono previsti costi aggiuntivi per la creazione dell'endpoint Amazon VPC quando si gestisce il security agent tramite. GuardDuty

  - È necessario che il nodo di lavoro disponga di un percorso di rete valido verso un endpoint `guardduty-data` VPC attivo. GuardDuty implementa il security agent sui tuoi cluster EKS. Amazon Elastic Kubernetes Service (Amazon EKS) coordinerà l'implementazione dell'agente di sicurezza sui nodi all'interno dei cluster EKS.
  - In base alla disponibilità IP, GuardDuty seleziona la sottorete per creare un endpoint VPC. Se utilizzi topologie di rete avanzate, devi verificare che la connettività sia possibile.
- Considerazione: attualmente, se utilizzi questa opzione, il monitoraggio del runtime EKS non crea un VPC condiviso.

Monitorare tutti i cluster EKS ed escludere cluster EKS selettivi

- Quando utilizzare questo approccio: utilizza questo approccio quando desideri gestire il security agent GuardDuty per tutti i cluster EKS del tuo account ma escludere i cluster EKS selettivi. Questo metodo utilizza un approccio[1] basato su tag in cui puoi assegnare tag ai cluster EKS per i quali non desideri ricevere gli eventi di runtime. La coppia chiave-valore del tag predefinito deve essere `GuardDutyManaged-false`.
- Impatto dell'utilizzo di questo approccio:
  - Questo approccio richiede l'attivazione della gestione automatica degli GuardDuty agenti solo dopo aver aggiunto tag ai cluster EKS che si desidera escludere dal monitoraggio.

    Pertanto, Gestisci l'agente di sicurezza tramite GuardDuty incide anche su questo approccio. Quando aggiungi tag prima di abilitare la gestione automatica degli GuardDuty agenti, non GuardDuty distribuirà né gestirà l'agente di sicurezza per i cluster EKS esclusi dal monitoraggio.
- Considerazioni:
  - È necessario aggiungere la coppia chiave-valore del tag come`GuardDutyManaged`: `false` per i cluster EKS selettivi prima di abilitare la configurazione automatizzata dell'agente, altrimenti, l'agente di GuardDuty sicurezza verrà distribuito su tutti i cluster EKS fino a quando non si utilizza il tag.
  - È necessario fare in modo che i tag vengano modificati solo da identità affidabili.

> **Important**
>
> Gestisci le autorizzazioni per modificare il valore del tag `GuardDutyManaged` per il cluster EKS utilizzando le policy di controllo dei servizi o le policy IAM. Per ulteriori informazioni, consulta le politiche di controllo dei servizi (SCP) nella Guida per l'AWS

Organizations utente o il controllo dell'accesso alle risorse nella Guida per AWS l'utente IAM.

- Assicurati di aggiungere la coppia chiave-valore `GuardDutyManaged-false` al momento della creazione di un cluster EKS potenzialmente nuovo che non desideri monitorare.
- La considerazione specificata per Monitorare tutti i cluster EKS vale anche per questo approccio.

Monitorare cluster EKS selettivi

- Quando utilizzare questo approccio: utilizza questo approccio quando desideri GuardDuty distribuire e gestire gli aggiornamenti del security agent solo per i cluster EKS selettivi del tuo account. Questo metodo utilizza un approccio[1] basato su tag in cui puoi assegnare tag al cluster EKS per il quale desideri ricevere gli eventi di runtime.
- Impatto dell'utilizzo di questo approccio:
  - Utilizzando i tag di inclusione, GuardDuty implementerà e gestirà automaticamente il security agent solo per i cluster EKS selettivi contrassegnati con `GuardDutyManaged` - come coppia chiave-valore. `true`
  - L'utilizzo di questo approccio avrà lo stesso impatto specificato per Monitorare tutti i cluster EKS.
- Considerazioni:
  - Se il valore del tag `GuardDutyManaged` non è impostato su `true`, il tag di inclusione non funzionerà come previsto e ciò potrebbe influire sul monitoraggio del cluster EKS.
  - Per garantire il monitoraggio dei cluster EKS selettivi, è necessario fare in modo che i tag vengano modificati solo da identità affidabili.

> **Important**
>
> Gestisci le autorizzazioni per modificare il valore del tag `GuardDutyManaged` per il cluster EKS utilizzando le policy di controllo dei servizi o le policy IAM. Per ulteriori informazioni, consulta le politiche di controllo dei servizi (SCP) nella Guida per l'AWS Organizations utente o il controllo dell'accesso alle AWS risorse nella Guida per l'utente IAM.

- Assicurati di aggiungere la coppia chiave-valore `GuardDutyManaged-false` al momento della creazione di un cluster EKS potenzialmente nuovo che non desideri monitorare.
- La considerazione specificata per Monitorare tutti i cluster EKS vale anche per questo approccio.

[1] Per ulteriori informazioni su come assegnare tag ai cluster EKS selettivi, consulta Assegnazione di tag alle risorse Amazon EKS nella Guida per l'utente di Amazon EKS.

Gestisci l'agente GuardDuty di sicurezza manualmente

- Quando utilizzare questo approccio: utilizza questo approccio quando desideri implementare e gestire manualmente il GuardDuty security agent su tutti i cluster EKS. Assicurati che il monitoraggio del runtime EKS sia abilitato per i tuoi account. L'agente GuardDuty di sicurezza potrebbe non funzionare come previsto se non abiliti EKS Runtime Monitoring.
- Impatto dell'utilizzo di questo approccio: sarà necessario coordinare l'implementazione del software GuardDuty Security Agent all'interno dei cluster EKS su tutti gli account e Regioni AWS laddove questa funzionalità sia disponibile.
- Considerazioni: è necessario mantenere un flusso di dati sicuro durante il monitoraggio e la risoluzione delle lacune di copertura man mano che vengono implementati nuovi cluster e carichi di lavoro.

Abilitazione del monitoraggio del GuardDuty runtime

Prima di abilitare il monitoraggio del runtime nel tuo account, assicurati che il tipo di risorsa per cui desideri monitorare gli eventi di runtime supporti i requisiti della piattaforma. Per ulteriori informazioni, consulta Prerequisiti.

Se avete utilizzato EKS Runtime Monitoring prima del lancio di EKS Runtime Monitoring, potete utilizzare le API per controllare e aggiornare la configurazione esistente per EKS Runtime Monitoring. È inoltre possibile migrare la configurazione esistente da EKS Runtime Monitoring a Runtime Monitoring. Per ulteriori informazioni, consulta Migrazione da EKS Runtime Monitoring a Runtime Monitoring.

> **Note**
>
> Attualmente, questa documentazione fornisce i passaggi per abilitare il monitoraggio del runtime per gli account e l'organizzazione solo tramite console. Puoi anche abilitare il monitoraggio del runtime utilizzando API Actions o AWS CLI for GuardDuty.

È possibile configurare Runtime Monitoring utilizzando i passaggi descritti nei seguenti argomenti.

Indice

- Abilitazione del monitoraggio del runtime per un account autonomo
- Per ambienti con più account
- Gestione degli agenti GuardDuty di sicurezza

Abilitazione del monitoraggio del runtime per un account autonomo

Console

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione, scegli Runtime Monitoring.
3. Nella scheda Configurazione, scegli Abilita per abilitare il monitoraggio del runtime per il tuo account.
4. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'istanza Amazon EC2, un cluster Amazon ECS o un cluster Amazon EKS, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

   Per abilitare l'agente di sicurezza GuardDuty

   - Gestione dell'agente di sicurezza automatizzato per l'istanza Amazon EC2
   - Gestione manuale dell'agente di sicurezza per l'istanza Amazon EC2
   - Gestione dell'agente di sicurezza automatizzato per Fargate (solo Amazon ECS)
   - Gestione automatica dell'agente di sicurezza per i cluster Amazon EKS
   - Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS

Per ambienti con più account

In ambienti con più account, solo l'account GuardDuty amministratore delegato può abilitare o disabilitare il Runtime Monitoring per gli account membro e gestire la configurazione automatica degli agenti per i tipi di risorse appartenenti agli account membro dell'organizzazione. GuardDuty Gli account membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce gli account dei membri utilizzando AWS Organizations. Per ulteriori informazioni sugli ambienti multi-account, consulta Gestione di più account.

Per l'account amministratore delegato GuardDuty

Per abilitare il monitoraggio del runtime per l'account amministratore delegato GuardDuty

1. Accedere AWS Management Console e aprire la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione, scegli Runtime Monitoring.
3. Nella scheda Configurazione, scegli Modifica nella sezione Configurazione di Runtime Monitoring.
4. Utilizzando Abilita per tutti gli account

   Se desideri abilitare il monitoraggio del runtime per tutti gli account che appartengono all'organizzazione, incluso l'account GuardDuty amministratore delegato, scegli Abilita per tutti gli account.
5. Utilizzando Configura gli account manualmente

   Se desideri abilitare il monitoraggio del runtime per ogni account membro singolarmente, scegli Configura gli account manualmente.

   - Scegli Abilita nella sezione Amministratore delegato (questo account).
6. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'istanza Amazon EC2, un cluster Amazon ECS o un cluster Amazon EKS, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

   Per abilitare l'agente di sicurezza GuardDuty

   - Gestione dell'agente di sicurezza automatizzato per l'istanza Amazon EC2
   - Gestione manuale dell'agente di sicurezza per l'istanza Amazon EC2
   - Gestione dell'agente di sicurezza automatizzato per Fargate (solo Amazon ECS)
   - Gestione automatica dell'agente di sicurezza per i cluster Amazon EKS
   - Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS

Per tutti gli account dei membri

Per abilitare il monitoraggio del runtime per tutti gli account membri dell'organizzazione

1. Accedere AWS Management Console e aprire la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando l'account GuardDuty amministratore delegato.
2. Nel riquadro di navigazione, scegli Runtime Monitoring.
3. Nella pagina Runtime Monitoring, nella scheda Configurazione, scegli Modifica nella sezione Configurazione di Runtime Monitoring.
4. Scegli Abilita per tutti gli account.
5. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'istanza Amazon EC2, un cluster Amazon ECS o un cluster Amazon EKS, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

   Per abilitare l'agente di sicurezza GuardDuty

   - Gestione dell'agente di sicurezza automatizzato per l'istanza Amazon EC2
   - Gestione manuale dell'agente di sicurezza per l'istanza Amazon EC2
   - Gestione dell'agente di sicurezza automatizzato per Fargate (solo Amazon ECS)
   - Gestione automatica dell'agente di sicurezza per i cluster Amazon EKS
   - Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS

Per tutti gli account membri attivi esistenti

Per abilitare il monitoraggio del runtime per gli account dei membri esistenti nell'organizzazione

1. Accedere AWS Management Console e aprire la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando l'account GuardDuty amministratore delegato dell'organizzazione.
2. Nel riquadro di navigazione, scegli Runtime Monitoring.
3. Nella pagina Runtime Monitoring, nella scheda Configurazione, puoi visualizzare lo stato corrente della configurazione di Runtime Monitoring.
4. Nel riquadro Runtime Monitoring, nella sezione Account dei membri attivi, scegli Azioni.

5. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
6. Scegli Conferma.
7. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'istanza Amazon EC2, un cluster Amazon ECS o un cluster Amazon EKS, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

   Per abilitare l'agente di sicurezza GuardDuty

   - Gestione dell'agente di sicurezza automatizzato per l'istanza Amazon EC2
   - Gestione manuale dell'agente di sicurezza per l'istanza Amazon EC2
   - Gestione dell'agente di sicurezza automatizzato per Fargate (solo Amazon ECS)
   - Gestione automatica dell'agente di sicurezza per i cluster Amazon EKS
   - Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS

> **Note**
>
> L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Abilita automaticamente il monitoraggio del runtime solo per gli account dei nuovi membri

Per abilitare il monitoraggio del runtime per gli account dei nuovi membri dell'organizzazione

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando l'account GuardDuty amministratore delegato designato dell'organizzazione.
2. Nel riquadro di navigazione, scegli Runtime Monitoring
3. Nella scheda Configurazione, scegli Modifica nella sezione Configurazione di Runtime Monitoring.
4. Scegli Configura gli account manualmente.
5. Seleziona Abilita automaticamente per i nuovi account membri.
6. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'istanza Amazon EC2, un cluster Amazon ECS o un cluster Amazon EKS, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

Per abilitare l'agente di sicurezza GuardDuty

- Gestione dell'agente di sicurezza automatizzato per l'istanza Amazon EC2
- Gestione manuale dell'agente di sicurezza per l'istanza Amazon EC2
- Gestione dell'agente di sicurezza automatizzato per Fargate (solo Amazon ECS)
- Gestione automatica dell'agente di sicurezza per i cluster Amazon EKS
- Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS

Solo per account di membri attivi selettivi

Per abilitare il monitoraggio del runtime per i singoli account dei membri attivi

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.
2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Nella pagina Account, rivedi automaticamente i valori nelle colonne Runtime Monitoring e Manage agent. Questi valori indicano se il monitoraggio del runtime e la gestione degli GuardDuty agenti sono abilitati o meno per l'account corrispondente.
4. Dalla tabella Account, selezionate l'account per il quale desiderate abilitare il Runtime Monitoring. Puoi scegliere più account alla volta.
5. Scegli Conferma.
6. Scegli Modifica piani di protezione. Scegliere l'operazione appropriata.
7. Scegli Conferma.
8. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'istanza Amazon EC2, un cluster Amazon ECS o un cluster Amazon EKS, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

   Per abilitare l'agente di sicurezza GuardDuty

   - Gestione dell'agente di sicurezza automatizzato per l'istanza Amazon EC2
   - Gestione manuale dell'agente di sicurezza per l'istanza Amazon EC2
   - Gestione dell'agente di sicurezza automatizzato per Fargate (solo Amazon ECS)
   - Gestione automatica dell'agente di sicurezza per i cluster Amazon EKS

- Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS

Gestione degli agenti GuardDuty di sicurezza

È possibile gestire il GuardDuty security agent per la risorsa che si desidera monitorare. Se desideri monitorare più di un tipo di risorsa, assicurati di gestire l' GuardDuty agente per quella risorsa.

> **Important**
>
> Quando lavori con un agente GuardDuty di sicurezza per un'istanza Amazon EC2, puoi installare e utilizzare l'agente sull'host sottostante all'interno di un cluster Amazon EKS. Se hai già implementato un agente di sicurezza su quel cluster EKS, sullo stesso host potrebbero essere in esecuzione due agenti di sicurezza contemporaneamente. Per informazioni su come GuardDuty funziona in questo scenario, consultaGestione dei doppi agenti di sicurezza.

I seguenti argomenti ti aiuteranno nei passaggi successivi per gestire il Security Agent.

Indice

- Utilizzo di VPC condiviso con agenti di sicurezza automatizzati
- Gestione dei doppi agenti di sicurezza installati su un host
- Gestione dell'agente di sicurezza automatizzato per l'istanza Amazon EC2
- Gestione manuale dell'agente di sicurezza per l'istanza Amazon EC2
- Gestione dell'agente di sicurezza automatizzato per Fargate (solo Amazon ECS)
- Gestione automatica dell'agente di sicurezza per i cluster Amazon EKS
- Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS

Utilizzo di VPC condiviso con agenti di sicurezza automatizzati

Quando si sceglie GuardDuty di gestire automaticamente il security agent, Runtime Monitoring supporta l'utilizzo di un VPC condiviso per Account AWS coloro che appartengono alla stessa organizzazione. AWS Organizations Per tuo conto, GuardDuty puoi impostare la policy degli endpoint Amazon VPC in base ai dettagli associati al VPC condiviso per la tua organizzazione.

Prima di questa versione, GuardDuty supportava l'uso di VPC condivisi solo quando si sceglieva di gestire il GuardDuty security agent manualmente.

Indice

- Come funziona
- Prerequisiti per l'utilizzo di un VPC condiviso
- Domande frequenti (FAQ)

Come funziona

Quando l'account proprietario del VPC condiviso abilita il monitoraggio del runtime e la configurazione automatica degli agenti per una qualsiasi delle risorse (Amazon EKS o (solo AWS Fargate Amazon ECS)), tutti i VPC condivisi diventano idonei per l'installazione automatica dell'endpoint Amazon VPC condiviso e del gruppo di sicurezza associato nell'account proprietario del VPC condiviso. GuardDuty recupera l'ID dell'organizzazione associato all'Amazon VPC condiviso.

Ora, le Account AWS persone che appartengono alla stessa organizzazione dell'account proprietario Amazon VPC condiviso possono condividere anche lo stesso endpoint Amazon VPC. GuardDuty crea il VPC condiviso quando l'account proprietario del VPC condiviso o l'account partecipante necessita di un endpoint Amazon VPC. Esempi di necessità di un endpoint Amazon VPC includono l' GuardDutyabilitazione, il monitoraggio del runtime, il monitoraggio del runtime EKS o il lancio di una nuova attività Amazon ECS-Fargate. Quando questi account abilitano il Runtime Monitoring e la configurazione automatizzata degli agenti per qualsiasi tipo di risorsa, GuardDuty creano un endpoint Amazon VPC e impostano la policy dell'endpoint con lo stesso ID dell'organizzazione dell'account proprietario del VPC condiviso. GuardDuty aggiunge un `GuardDutyManaged` tag e lo imposta `true` per l'endpoint Amazon VPC che lo crea. GuardDuty Se l'account proprietario di Amazon VPC condiviso non ha abilitato il monitoraggio del runtime o la configurazione automatica degli agenti per nessuna delle risorse, non GuardDuty imposterà la policy degli endpoint di Amazon VPC. Per informazioni sulla configurazione del Runtime Monitoring e sulla gestione automatica del security agent nell'account proprietario del VPC condiviso, consulta. Abilitazione del monitoraggio del GuardDuty runtime

Ciascuno degli account che utilizzano la stessa policy per gli endpoint di Amazon VPC viene chiamato AWS account partecipante dell'Amazon VPC condiviso associato.

L'esempio seguente mostra la politica degli endpoint VPC predefinita dell'account proprietario del VPC condiviso e dell'account partecipante. `aws:PrincipalOrgID`Mostrerà l'ID dell'organizzazione

associato alla risorsa VPC condivisa. L'uso di questa politica è limitato agli account dei partecipanti presenti nell'organizzazione dell'account del proprietario.

Example

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "*",
            "Resource": "*",
            "Effect": "Allow",
            "Principal": "*"
        },
        {
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalOrgID": "o-abcdef0123"
                }
            },
            "Action": "*",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "*"
        }
    ]
}
```

Prerequisiti per l'utilizzo di un VPC condiviso

Prerequisiti per la configurazione iniziale

Esegui i seguenti passaggi se desideri diventare il proprietario del VPC condiviso: Account AWS

1. Creazione di un'organizzazione: crea un'organizzazione seguendo i passaggi descritti in Creazione e gestione di un'organizzazione nella Guida per l'AWS Organizations utente.

   Per informazioni sull'aggiunta o la rimozione degli account dei membri, consulta Gestione Account AWS nell'organizzazione.
2. Creazione di una risorsa VPC condivisa: puoi creare una risorsa VPC condivisa dall'account del proprietario. Per ulteriori informazioni, consulta Condivisione del VPC con altri account nella Guida per l'utente di Amazon VPC.

Prerequisiti specifici per il monitoraggio del runtime GuardDuty

L'elenco seguente fornisce i prerequisiti specifici per: GuardDuty

- L'account proprietario del VPC condiviso e l'account partecipante possono appartenere a organizzazioni diverse in. GuardDuty Tuttavia, devono appartenere alla stessa organizzazione in AWS Organizations. Ciò è necessario per GuardDuty creare un endpoint Amazon VPC e un gruppo di sicurezza per il VPC condiviso. Per informazioni su come funzionano i VPC condivisi, consulta Condividi il tuo VPC con altri account nella Amazon VPC User Guide.
- Abilita Runtime Monitoring o EKS Runtime Monitoring e la configurazione GuardDuty automatizzata degli agenti per qualsiasi risorsa nell'account proprietario del VPC condiviso e nell'account partecipante. Per ulteriori informazioni, consulta Abilitazione del monitoraggio del runtime.

  Se hai già completato queste configurazioni, continua con il passaggio successivo.
- Quando lavori con un'attività Amazon EKS o Amazon ECS (AWS Fargate solo), assicurati di scegliere la risorsa VPC condivisa associata all'account del proprietario e di selezionarne le sottoreti.

Domande frequenti (FAQ)

L'elenco seguente fornisce i passaggi per la risoluzione dei problemi relativi alle domande frequenti quando si utilizza una risorsa VPC condivisa con la configurazione GuardDuty automatica degli agenti abilitata in Runtime Monitoring:

Sto già utilizzando Runtime Monitoring (o EKS Runtime Monitoring). Come posso abilitare il VPC condiviso?

Per informazioni sui prerequisiti per creare un VPC condiviso, vedere. Prerequisiti

Quando sia l'account proprietario del VPC condiviso che l'account partecipante soddisfano i prerequisiti, GuardDuty tenterà di impostare automaticamente la policy degli endpoint di Amazon VPC.

Se prima di questa versione hai Account AWS riscontrato un problema di copertura relativo al mancato supporto del VPC condiviso, segui i prerequisiti. Quando il tipo di risorsa (attività Amazon EKS o Amazon ECS (AWS Fargate solo)) richiama il requisito di un endpoint VPC condiviso, GuardDuty tenterà di impostare la nuova policy degli endpoint VPC.

In qualità di proprietario di un account VPC condiviso, voglio che la policy degli endpoint VPC condivisi sia limitata a un sottoinsieme di account partecipanti nella mia organizzazione. Come posso farlo?

Se hai un `true` tag`GuardDutyManaged`: associato all'endpoint, rimuovilo. Ciò impedisce GuardDuty di tentare di modificare o sovrascrivere la policy degli endpoint VPC del VPC condiviso.

Per ulteriori informazioni, consulta Controllare l'accesso agli endpoint VPC utilizzando le policy degli endpoint.

Perché l'endpoint VPC condiviso viene modificato da a? **`aws:PrincipalAccount`** **`aws:PrincipalOrgId`** Come posso evitarlo?

Quando GuardDuty rileva che il VPC è condiviso da più account della stessa organizzazione AWS Organizations in GuardDuty , tenta di modificare la policy per specificare l'ID dell'organizzazione.

Per evitare che ciò accada, rimuovi il `true` tag`GuardDutyManaged`: dall'endpoint VPC condiviso. Ciò impedisce GuardDuty di tentare di modificare o sovrascrivere la policy degli endpoint VPC del VPC condiviso.

Cosa succede quando l'account proprietario del VPC condiviso o uno degli account dei partecipanti disabilita il Runtime Monitoring (GuardDuty o EKS Runtime Monitoring)?

Quando l'account proprietario del VPC condiviso disabilita GuardDuty o Runtime Monitoring (o EKS Runtime Monitoring), GuardDuty verifica se qualsiasi tipo di risorsa appartenente all'account partecipante ha utilizzato l'endpoint VPC condiviso o se qualsiasi account partecipante ha mai abilitato la gestione degli agenti per qualsiasi tipo di risorsa. GuardDuty In caso affermativo, GuardDuty non eliminerà l'endpoint VPC e il gruppo di sicurezza.

Se l'account partecipante VPC condiviso disabilita il monitoraggio del runtime GuardDuty o il monitoraggio del runtime (o EKS Runtime Monitoring), non vi è alcun impatto sull'account proprietario del VPC condiviso e l'account proprietario non eliminerà né la risorsa VPC condivisa né il gruppo di sicurezza.

Come posso eliminare la risorsa VPC condivisa? Quale sarà il suo impatto?

In qualità di account proprietario di un VPC condiviso, puoi eliminare la risorsa VPC condivisa anche quando viene utilizzata dal tuo account o da uno degli account partecipanti al Runtime Monitoring. Per informazioni sull'eliminazione del VPC condiviso e sulla comprensione del suo impatto, consulta. To delete VPC endpoint

Gestione dei doppi agenti di sicurezza installati su un host

Le istanze Amazon EC2 possono supportare diversi tipi di carichi di lavoro. Quando configuri un agente di sicurezza automatizzato su un'istanza Amazon EC2, la stessa istanza EC2 potrebbe avere un altro agente di sicurezza tramite EKS.

Panoramica

Prendi in considerazione uno scenario in cui hai abilitato il monitoraggio del runtime. Ora puoi abilitare l'agente automatizzato per Amazon EKS tramite GuardDuty. Hai anche abilitato l'agente automatizzato per Amazon EC2. Può succedere che sullo stesso host sottostante vengano installati due agenti di sicurezza, uno per Amazon EKS e l'altro per Amazon EC2. Ciò potrebbe comportare l'esecuzione di due agenti di sicurezza all'interno dello stesso host, che raccolgono eventi di runtime e li inviano a GuardDuty, generando potenzialmente risultati duplicati.

Impatto

- Quando più di un security agent è in esecuzione sullo stesso host, il tuo account potrebbe avere il doppio delle esigenze di elaborazione della CPU e della memoria. Per informazioni sui limiti di CPU e memoria per ogni tipo di risorsa, vedi Prerequisiti for that resource.
- GuardDuty ha progettato la funzionalità Runtime Monitoring in modo tale che, anche in caso di sovrapposizione di due security agent che raccolgono eventi di runtime dallo stesso host sottostante, all'account venga addebitato solo un flusso di eventi di runtime.

Come GuardDuty gestisce più agenti

GuardDuty rileva quando due security agent sono in esecuzione sullo stesso host e ne designa solo uno come agente di sicurezza che raccoglie attivamente gli eventi di runtime. Il secondo agente consumerà risorse di sistema minime in modo da prevenire qualsiasi impatto sulle prestazioni delle applicazioni.

GuardDuty considera i seguenti scenari:

- Quando un'istanza EC2 rientra nell'ambito degli agenti di sicurezza di Amazon EKS e Amazon EC2, l'agente di sicurezza EKS ha la priorità. Ciò si applica solo quando utilizzi il security agent v1.1.0 o successivo per Amazon EC2. Le versioni precedenti degli agenti continueranno a funzionare e a raccogliere eventi di runtime perché le versioni precedenti degli agenti non sono influenzate dalla prioritizzazione.

- Quando sia Amazon EKS che Amazon EC2 dispongono di agenti di sicurezza GuardDuty gestiti e l'istanza Amazon EC2 è gestita anche tramite SSM, entrambi gli agenti di sicurezza verranno installati a livello di host. Una volta installati gli agenti, GuardDuty decide quale agente di sicurezza continuerà a funzionare. Quando entrambi i security agent sono in esecuzione, alla fine solo uno di essi raccoglierà gli eventi di runtime.
- Quando i security agent associati sia a EC2 che a EKS vengono eseguiti contemporaneamente, GuardDuty potrebbero generare risultati duplicati solo durante il periodo di sovrapposizione.

  Questo può accadere quando:

  - Gli agenti di sicurezza per EC2 e EKS sono configurati tramite GuardDuty (automaticamente) o
  - La tua risorsa Amazon EKS dispone di un agente di sicurezza automatizzato.
- Quando l'agente di sicurezza EKS è già in esecuzione, se lo distribuisci manualmente sullo stesso host sottostante e soddisfi tutti i prerequisiti, GuardDuty potresti non installare un secondo agente di sicurezza.

Gestione dell'agente di sicurezza automatizzato per l'istanza Amazon EC2

Migrazione da un agente manuale di Amazon EC2 a un agente automatizzato

Questa sezione si applica a Account AWS chi in precedenza gestiva manualmente il Security Agent e ora desidera utilizzare la configurazione GuardDuty automatizzata dell'agente. Se ciò non ti riguarda, continua con la configurazione del security agent per il tuo account.

Quando abiliti l'agente GuardDuty automatizzato, GuardDuty gestisce l'agente di sicurezza per tuo conto. Per informazioni sui passaggi GuardDuty necessari, consultaUtilizza la configurazione automatica degli agenti (scelta consigliata).

Pulizia delle risorse

Eliminare l'associazione SSM

- Elimina qualsiasi associazione SSM che potresti aver creato durante la gestione manuale del security agent per Amazon EC2. Per ulteriori informazioni, consulta Eliminazione delle associazioni.
- Questo viene fatto in modo che GuardDuty possa assumere il controllo della gestione delle azioni SSM indipendentemente dal fatto che si utilizzino agenti automatici a livello di account o di istanza (utilizzando tag di inclusione o esclusione). Per ulteriori informazioni su cosa possono

essere eseguite le azioni SSM, GuardDuty consulta. Autorizzazioni di ruolo collegate al servizio per GuardDuty

- Quando si elimina un'associazione SSM creata in precedenza per la gestione manuale del Security Agent, potrebbe verificarsi un breve periodo di sovrapposizione quando si GuardDuty crea un'associazione SSM per la gestione automatica del Security Agent. Durante questo periodo, potrebbero verificarsi conflitti basati sulla pianificazione SSM. Per ulteriori informazioni, consulta la pianificazione SSM di Amazon EC2.

Gestisci i tag di inclusione ed esclusione per le tue istanze Amazon EC2

- Tag di inclusione: quando non abiliti la configurazione GuardDuty automatizzata degli agenti ma contrassegni una qualsiasi delle tue istanze Amazon EC2 con un tag di inclusione (`GuardDutyManaged:true`), GuardDuty crea un'associazione SSM che installerà e gestirà il security agent sulle istanze EC2 selezionate. Si tratta di un comportamento previsto che ti aiuta a gestire il security agent solo su istanze EC2 selezionate. Per ulteriori informazioni, consulta Come funziona il monitoraggio del runtime con le istanze Amazon EC2.

  Per GuardDuty impedire l'installazione e la gestione del security agent, rimuovi il tag di inclusione da queste istanze EC2. Per ulteriori informazioni, consulta Aggiungere ed eliminare tag nella Guida per l'utente di Amazon EC2 per le istanze Linux.
- Tag di esclusione: se desideri abilitare la configurazione GuardDuty automatica degli agenti per tutte le istanze EC2 del tuo account, assicurati che nessuna istanza EC2 sia etichettata con un tag di esclusione (:). `GuardDutyManaged false`

Configurazione dell'agente per un account autonomo GuardDuty

Configure for all instances

Per configurare GuardDuty Security Agent per tutte le istanze del tuo account standalone

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione, scegli Runtime Monitoring.
3. Nella scheda Configurazione, scegli Modifica.
4. Nella sezione EC2, scegli Abilita.
5. Selezionare Salva.
6. Puoi verificare che l'associazione SSM che GuardDuty crea installerà e gestirà il security agent su tutte le risorse EC2 appartenenti al tuo account.

a. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.

b. Apri la scheda Targets per l'associazione SSM (`GuardDutyRuntimeMonitoring-do-not-delete`). Osservate che il tasto Tag appare come InstanceIds.

Using inclusion tag in selected instances

Per configurare l'agente GuardDuty di sicurezza per istanze Amazon EC2 selezionate

1. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `true` tag`GuardDutyManaged`: alle istanze che desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.
3. Puoi verificare che l'associazione SSM che GuardDuty crea installerà e gestirà il security agent solo sulle risorse EC2 etichettate con i tag di inclusione.

   Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.

   - Apri la scheda Target per l'associazione SSM che viene creata (`GuardDutyRuntimeMonitoring-do-not-delete`). La chiave Tag appare come tag: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Assicurati di aggiungere il tag di esclusione alle istanze Amazon EC2 prima di avviarle. Quando abiliti la configurazione automatizzata degli agenti per Amazon EC2, qualsiasi istanza EC2 che viene avviata senza un tag di esclusione sarà coperta dalla configurazione automatizzata dell'agente. GuardDuty

Per configurare l'agente GuardDuty di sicurezza per istanze Amazon EC2 selezionate

1. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `false` tag`GuardDutyManaged`: alle istanze in cui non desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.
3. Affinché i tag di esclusione siano disponibili nei metadati dell'istanza, effettuate le seguenti operazioni:

   a. Nella scheda Dettagli dell'istanza, visualizza lo stato di Consenti i tag nei metadati dell'istanza.

      Se attualmente è Disabilitato, utilizza i seguenti passaggi per modificare lo stato in Abilitato. In caso contrario, puoi ignorare questo passaggio.

   b. Seleziona l'istanza per la quale desideri consentire i tag.

   c. Nel menu Azioni, scegli Impostazioni istanza.

   d. Scegli Consenti tag nei metadati dell'istanza.

   e. In Accesso ai tag nei metadati dell'istanza, seleziona Consenti.

   f. Selezionare Salva.
4. Dopo aver aggiunto il tag di esclusione, esegui gli stessi passaggi specificati nella scheda Configura per tutte le istanze.

Ora puoi valutare il runtime. Copertura per l'istanza Amazon EC2

Configurazione GuardDuty dell'agente in un ambiente con più account

Per account amministratore delegato GuardDuty

Configure for all instances

Se hai scelto Abilita per tutti gli account per il monitoraggio del runtime, scegli una delle seguenti opzioni per l'account GuardDuty amministratore delegato:

- Opzione 1

  In Configurazione automatica dell'agente, nella sezione EC2, seleziona Abilita per tutti gli account.

- Opzione 2
  - In Configurazione automatizzata dell'agente, nella sezione EC2, seleziona Configura gli account manualmente.
  - In Amministratore delegato (questo account), scegli Abilita.
- Selezionare Salva.

Se hai scelto Configura gli account manualmente per il monitoraggio del runtime, procedi nel seguente modo:

- In Configurazione automatizzata degli agenti, nella sezione EC2, seleziona Configura gli account manualmente.
- In Amministratore delegato (questo account), scegli Abilita.
- Selezionare Salva.

Indipendentemente dall'opzione scelta per abilitare la configurazione automatica dell'agente per l'account GuardDuty amministratore delegato, puoi verificare che l'associazione SSM GuardDuty creata installerà e gestirà il security agent su tutte le risorse EC2 appartenenti a questo account.

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Apri la scheda Targets per l'associazione SSM (`GuardDutyRuntimeMonitoring-do-not-delete`). Osservate che il tasto Tag appare come InstanceIds.

Using inclusion tag in selected instances

Per configurare GuardDuty l'agente per istanze Amazon EC2 selezionate

1. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `true` tag`GuardDutyManaged`: alle istanze che desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.

   L'aggiunta di questo tag consentirà GuardDuty di installare e gestire il security agent per queste istanze EC2 selezionate. Non è necessario abilitare la configurazione automatica degli agenti in modo esplicito.

3. È possibile verificare che l'associazione SSM GuardDuty creata installi e gestisca il security agent solo sulle risorse EC2 etichettate con i tag di inclusione.

   Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.

   - Apri la scheda Target per l'associazione SSM che viene creata (`GuardDutyRuntimeMonitoring-do-not-delete`). La chiave Tag appare come tag: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Assicurati di aggiungere il tag di esclusione alle istanze Amazon EC2 prima di avviarle. Quando abiliti la configurazione automatizzata degli agenti per Amazon EC2, qualsiasi istanza EC2 che viene avviata senza un tag di esclusione sarà coperta dalla configurazione automatizzata dell'agente. GuardDuty

Per configurare GuardDuty l'agente per istanze Amazon EC2 selezionate

1. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `false` tag`GuardDutyManaged`: alle istanze in cui non desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.
3. Affinché i tag di esclusione siano disponibili nei metadati dell'istanza, effettuate le seguenti operazioni:

   a. Nella scheda Dettagli dell'istanza, visualizza lo stato di Consenti i tag nei metadati dell'istanza.

      Se attualmente è Disabilitato, utilizza i seguenti passaggi per modificare lo stato in Abilitato. In caso contrario, puoi ignorare questo passaggio.

   b. Nel menu Azioni, scegli Impostazioni istanza.

   c. Scegli Consenti tag nei metadati dell'istanza.

4. Dopo aver aggiunto il tag di esclusione, esegui gli stessi passaggi specificati nella scheda Configura per tutte le istanze.

Ora puoi valutare il runtime. Copertura per l'istanza Amazon EC2

Attivazione automatica per tutti gli account dei membri

> **Note**
>
> L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Configure for all instances

I passaggi seguenti presuppongono che tu abbia scelto Abilita per tutti gli account nella sezione Runtime Monitoring:

1. Scegli Abilita per tutti gli account nella sezione Configurazione automatica degli agenti per Amazon EC2.
2. Puoi verificare che l'associazione SSM che GuardDuty crea (`GuardDutyRuntimeMonitoring-do-not-delete`) installi e gestisca il security agent su tutte le risorse EC2 appartenenti a questo account.
   a. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
   b. Apri la scheda Targets per l'associazione SSM. Osserva che il tasto Tag appare come InstanceIds.

Using inclusion tag in selected instances

Per configurare GuardDuty l'agente per istanze Amazon EC2 selezionate

1. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `true` tag`GuardDutyManaged`: alle istanze EC2 che desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Aggiungere un tag a una singola risorsa.

L'aggiunta di questo tag consentirà GuardDuty di installare e gestire il security agent per queste istanze EC2 selezionate. Non è necessario abilitare la configurazione automatica degli agenti in modo esplicito.

3. Puoi verificare che l'associazione SSM che GuardDuty crea installerà e gestirà il security agent su tutte le risorse EC2 appartenenti al tuo account.

   a. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.

   b. Apri la scheda Targets per l'associazione SSM (`GuardDutyRuntimeMonitoring-do-not-delete`). Osservate che il tasto Tag appare come InstanceIds.

Using exclusion tag in selected instances

> **Note**
>
> Assicurati di aggiungere il tag di esclusione alle istanze Amazon EC2 prima di avviarle. Quando abiliti la configurazione automatizzata degli agenti per Amazon EC2, qualsiasi istanza EC2 che viene avviata senza un tag di esclusione sarà coperta dalla configurazione automatizzata dell'agente. GuardDuty

Per configurare l'agente GuardDuty di sicurezza per istanze Amazon EC2 selezionate

1. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `false` tag`GuardDutyManaged`: alle istanze in cui non desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.
3. Affinché i tag di esclusione siano disponibili nei metadati dell'istanza, effettuate le seguenti operazioni:

   a. Nella scheda Dettagli dell'istanza, visualizza lo stato di Consenti i tag nei metadati dell'istanza.

   Se attualmente è Disabilitato, utilizza i seguenti passaggi per modificare lo stato in Abilitato. In caso contrario, puoi ignorare questo passaggio.

b. Nel menu Azioni, scegli Impostazioni istanza.

c. Scegli Consenti tag nei metadati dell'istanza.

4. Dopo aver aggiunto il tag di esclusione, esegui gli stessi passaggi specificati nella scheda Configura per tutte le istanze.

Ora puoi valutare il runtime. Copertura per l'istanza Amazon EC2

Attivazione automatica solo per gli account dei nuovi membri

L'account GuardDuty amministratore delegato può impostare la configurazione automatica dell'agente per la risorsa Amazon EC2 in modo che si abiliti automaticamente per i nuovi account membri quando entrano a far parte dell'organizzazione.

Configure for all instances

I passaggi seguenti presuppongono che tu abbia selezionato Abilita automaticamente gli account dei nuovi membri nella sezione Runtime Monitoring:

1. Nel riquadro di navigazione, scegli Runtime Monitoring.
2. Nella pagina Runtime Monitoring, scegli Modifica.
3. Seleziona Abilita automaticamente per i nuovi account membri. Questo passaggio garantisce che ogni volta che un nuovo account si unisce alla tua organizzazione, la configurazione automatizzata degli agenti per Amazon EC2 venga abilitata automaticamente per l'account. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa selezione.
4. Selezionare Salva.

Quando un nuovo account membro si unisce all'organizzazione, questa configurazione verrà abilitata automaticamente per lui. GuardDuty Per gestire l'agente di sicurezza per le istanze Amazon EC2 che appartengono a questo nuovo account membro, assicurati che tutti i prerequisiti Per l'istanza EC2 siano soddisfatti.

Quando viene creata un'associazione SSM (`GuardDutyRuntimeMonitoring-do-not-delete`), puoi verificare che l'associazione SSM installi e gestisca il security agent su tutte le istanze EC2 appartenenti al nuovo account membro.

- Apri la console all'indirizzo https://console.aws.amazon.com/systems-manager/ AWS Systems Manager .
- Apri la scheda Targets per l'associazione SSM. Osserva che il tasto Tag appare come InstanceIds.

Using inclusion tag in selected instances

Per configurare il GuardDuty Security Agent per istanze selezionate nel tuo account

1. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `true` tag`GuardDutyManaged`: alle istanze che desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.

   L'aggiunta di questo tag consentirà GuardDuty di installare e gestire il security agent per queste istanze selezionate. Non è necessario abilitare esplicitamente la configurazione automatica dell'agente.
3. È possibile verificare che l'associazione SSM GuardDuty creata installi e gestisca il security agent solo sulle risorse EC2 etichettate con i tag di inclusione.

   a. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.

   b. Apri la scheda Target per l'associazione SSM che viene creata. La chiave Tag appare come tag: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Assicurati di aggiungere il tag di esclusione alle istanze Amazon EC2 prima di avviarle. Quando abiliti la configurazione automatizzata degli agenti per Amazon EC2, qualsiasi istanza EC2 che viene avviata senza un tag di esclusione sarà coperta dalla configurazione automatizzata dell'agente. GuardDuty

Per configurare l'agente GuardDuty di sicurezza per istanze specifiche nel tuo account autonomo

1. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `false` tag`GuardDutyManaged`: alle istanze in cui non desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.
3. Affinché i tag di esclusione siano disponibili nei metadati dell'istanza, effettuate le seguenti operazioni:

   a. Nella scheda Dettagli dell'istanza, visualizza lo stato di Consenti i tag nei metadati dell'istanza.

      Se attualmente è Disabilitato, utilizza i seguenti passaggi per modificare lo stato in Abilitato. In caso contrario, puoi ignorare questo passaggio.

   b. Nel menu Azioni, scegli Impostazioni istanza.

   c. Scegli Consenti tag nei metadati dell'istanza.
4. Dopo aver aggiunto il tag di esclusione, esegui gli stessi passaggi specificati nella scheda Configura per tutte le istanze.

Ora puoi valutare il runtime. Copertura per l'istanza Amazon EC2

Solo account membri selettivi

Configure for all instances

1. Nella pagina Account, seleziona uno o più account per i quali desideri abilitare la configurazione dell'agente Runtime Monitoring-Automated (Amazon EC2). Assicurati che gli account selezionati in questo passaggio abbiano già abilitato il Runtime Monitoring.
2. Da Modifica piani di protezione, scegli l'opzione appropriata per abilitare la configurazione automatica degli agenti di Runtime Monitoring-Automated (Amazon EC2).
3. Scegli Conferma.

Using inclusion tag in selected instances

Per configurare l'agente di GuardDuty sicurezza per istanze selezionate

1. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `true` tag`GuardDutyManaged`: alle istanze che desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.

   L'aggiunta di questo tag consentirà di GuardDuty gestire l'agente di sicurezza per le istanze Amazon EC2 con tag. Non è necessario abilitare esplicitamente la configurazione automatica degli agenti (Runtime Monitoring - Automated agent configuration (EC2).

Using exclusion tag in selected instances

> **Note**
>
> Assicurati di aggiungere il tag di esclusione alle istanze Amazon EC2 prima di avviarle. Quando abiliti la configurazione automatizzata degli agenti per Amazon EC2, qualsiasi istanza EC2 che viene avviata senza un tag di esclusione sarà coperta dalla configurazione automatizzata dell'agente. GuardDuty

Per configurare l'agente di GuardDuty sicurezza per istanze selezionate

1. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `false` tag`GuardDutyManaged`: alle istanze EC2 che non desideri GuardDuty monitorare o rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Aggiungere un tag a una singola risorsa.
3. Affinché i tag di esclusione siano disponibili nei metadati dell'istanza, effettuate le seguenti operazioni:

   a. Nella scheda Dettagli dell'istanza, visualizza lo stato di Consenti i tag nei metadati dell'istanza.

Se attualmente è Disabilitato, utilizza i seguenti passaggi per modificare lo stato in Abilitato. In caso contrario, puoi ignorare questo passaggio.

b. Nel menu Azioni, scegli Impostazioni istanza.

c. Scegli Consenti tag nei metadati dell'istanza.

4. Dopo aver aggiunto il tag di esclusione, esegui gli stessi passaggi specificati nella scheda Configura per tutte le istanze.

Ora puoi valutare. Copertura per l'istanza Amazon EC2

Gestione manuale dell'agente di sicurezza per l'istanza Amazon EC2

Dopo aver abilitato il Runtime Monitoring, dovrai installare il GuardDuty security agent manualmente. Installando l'agente, GuardDuty riceverà gli eventi di runtime dalle istanze Amazon EC2.

Per gestire il GuardDuty security agent, devi creare un endpoint Amazon VPC e quindi seguire i passaggi per installare il security agent manualmente.

Creazione manuale di un endpoint Amazon VPC

Prima di poter installare il GuardDuty security agent, devi creare un endpoint Amazon Virtual Private Cloud (Amazon VPC). Questo ti aiuterà a GuardDuty ricevere gli eventi di runtime delle tue istanze Amazon EC2.

> **Note**
>
> Non sono previsti costi aggiuntivi per l'utilizzo dell'endpoint VPC.

Per creare un endpoint Amazon VPC

1. Accedi AWS Management Console e apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, in VPC private cloud, scegli Endpoints.
3. Scegliere Create Endpoint (Crea endpoint).
4. Nella pagina Crea endpoint per Categoria servizio, scegli Altri servizi endpoint.
5. Per Nome servizio, inserisci **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**.

Assicurati di sostituire *us-east-1* con il tuo. Regione AWS Questa deve essere la stessa regione dell'istanza Amazon EC2 che appartiene all'ID del tuo AWS account.

6. Scegli Verifica del servizio.
7. Dopo aver verificato con successo il nome del servizio, scegli il VPC in cui risiede l'istanza. Aggiungi la seguente policy per limitare l'utilizzo degli endpoint Amazon VPC solo all'account specificato. Con la `Condition` dell'organizzazione fornita sotto a questa policy, puoi aggiornare la policy seguente per limitare l'accesso all'endpoint. Per fornire il supporto degli endpoint Amazon VPC a ID di account specifici della tua organizzazione, consulta. Organization condition to restrict access to your endpoint

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
 ]
}
```

L'ID account di `aws:PrincipalAccount` deve corrispondere all'account contenente il VPC e l'endpoint VPC. L'elenco seguente mostra come condividere l'endpoint VPC con altri AWS ID account:

- Per specificare più account per accedere all'endpoint VPC, sostituiscilo `"aws:PrincipalAccount: "111122223333"` con il seguente blocco:

```
"aws:PrincipalAccount": [
          "666666666666",
          "555555555555"
      ]
```

Assicurati di sostituire gli ID AWS account con gli ID account di quegli account che devono accedere all'endpoint VPC.

- Per consentire a tutti i membri di un'organizzazione di accedere all'endpoint VPC, sostituiscilo `"aws:PrincipalAccount: "111122223333"` con la seguente riga:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

Assicurati di sostituire l'organizzazione *o-abcdef0123* con l'ID della tua organizzazione.

- Per limitare l'accesso a una risorsa tramite un ID dell'organizzazione, aggiungi il tuo alla politica. `ResourceOrgID` Per ulteriori informazioni, consulta la sezione `aws:ResourceOrgID` nella Guida per l'utente di IAM.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. In Impostazioni aggiuntive, scegli Abilita nome DNS.
9. In Sottoreti, scegli le sottoreti in cui risiede l'istanza.
10. In Gruppi di sicurezza, scegli un gruppo di sicurezza con la porta in ingresso 443 abilitata dal tuo VPC (o dalla tua istanza Amazon EC2). Se non disponi già di un gruppo di sicurezza con una porta in ingresso 443 abilitata, consulta Creare un gruppo di sicurezza nella Amazon EC2 User Guide for Linux Instances.

    Se c'è un problema durante la limitazione delle autorizzazioni in ingresso al tuo VPC (o istanza), fornisci il supporto alla porta 443 in ingresso da qualsiasi indirizzo IP. `(0.0.0.0/0)`

Installazione manuale del security agent

GuardDuty fornisce i due metodi seguenti per installare il GuardDuty security agent sulle istanze Amazon EC2:

- Metodo 1 AWS Systems Manager - Utilizzo: questo metodo richiede la gestione dell'istanza Amazon EC2. AWS Systems Manager

- Metodo 2 - Utilizzando script di installazione RPM: puoi utilizzare questo metodo indipendentemente dal fatto che le tue istanze Amazon EC2 siano gestite o meno. AWS Systems Manager

Metodo 1: utilizzando AWS Systems Manager

Per utilizzare questo metodo, assicurati che le tue istanze Amazon EC2 siano AWS Systems Manager gestite e quindi installa l'agente.

AWS Systems Manager istanza Amazon EC2 gestita

Utilizza i seguenti passaggi per gestire le tue istanze AWS Systems Manager Amazon EC2.

- AWS Systems Managerti aiuta a gestire AWS applicazioni e risorse end-to-end e a consentire operazioni sicure su larga scala.

  Per gestire le istanze Amazon EC2 con AWS Systems Manager, consulta Configurazione delle istanze di Systems Manager per Amazon EC2 nella Guida per l'utente.AWS Systems Manager
- La tabella seguente mostra i nuovi documenti gestiti: GuardDuty AWS Systems Manager

Nome del documento	Tipo di documento	Scopo
`AmazonGuardDuty-RuntimeMonitoringSsmPlugin`	Distributor	Per impacchettare il GuardDuty security agent.
`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`	Comando	Per eseguire lo script di installazione/disinstallazione per installare il security agent. GuardDuty

Per ulteriori informazioni AWS Systems Manager, consulta i documenti di Amazon EC2 Systems Manager nella Guida per AWS Systems Manager l'utente.

Per installare l' GuardDuty agente per l'istanza Amazon EC2 utilizzando AWS Systems Manager

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel riquadro di navigazione, scegli Documenti
3. In Owned by Amazon, scegli`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`.
4. Scegliere Run Command.
5. Inserisci i seguenti parametri Run Command
   - Azione: Scegli Installa.
   - Tipo di installazione: scegli Installa o Disinstalla.
   - Valore: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`
   - Versione: se rimane vuoto, otterrai la versione più recente del GuardDuty Security Agent. Per ulteriori informazioni sulle versioni di rilascio,GuardDuty agente di sicurezza per istanze Amazon EC2.
6. Seleziona l'istanza Amazon EC2 di destinazione. Puoi selezionare una o più istanze Amazon EC2. Per ulteriori informazioni, consulta AWS Systems Manager Esecuzione di comandi dalla console nella Guida per l'AWS Systems Manager utente
7. Verifica se l'installazione dell' GuardDuty agente è integra. Per ulteriori informazioni, consulta Convalida dello stato di installazione del GuardDuty Security Agent.

Metodo 2: utilizzando gli script di installazione RPM

> **Important**
>
> Consigliamo vivamente di verificare la firma RPM del GuardDuty Security Agent prima di installarla sul computer.

1. Verifica la firma RPM del GuardDuty Security Agent

a. Scarica la chiave pubblica appropriata, la firma di x86_64 RPM, la firma di arm64 RPM e il collegamento di accesso corrispondente agli script RPM ospitati nei bucket Amazon S3

   È possibile utilizzare i seguenti modelli per creare la chiave pubblica, la firma di x86_64 RPM, la firma di arm64 RPM e il collegamento di accesso corrispondente agli script RPM. Sostituite il valore dell'ID dell' AWS account e Regione AWS la versione dell'agente per accedere agli GuardDuty script RPM.

   - Chiave pubblica:

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/publickey.pem
     ```

   - GuardDuty firma RPM dell'agente di sicurezza:

     Firma di x86_64 RPM

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/
     amazon-guardduty-agent-1.1.0.x86_64.sig
     ```

     Firma di arm64 RPM

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/
     amazon-guardduty-agent-1.1.0.arm64.sig
     ```

   - Accedi ai link agli script RPM nel bucket Amazon S3:

     Link di accesso per x86_64 RPM

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/
     amazon-guardduty-agent-1.1.0.x86_64.rpm
     ```

     Link di accesso per arm64 RPM

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/
     amazon-guardduty-agent-1.1.0.arm64.rpm
     ```

   Nel seguente comando per scaricare la chiave pubblica appropriata, la firma di x86_64 RPM, la firma di arm64 RPM e il collegamento di accesso corrispondente agli script RPM

ospitati nei bucket Amazon S3, assicurati di sostituire l'ID dell'account con l'ID appropriato e la regione con la regione corrente. Account AWS

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
x86_64/amazon-guardduty-agent-1.1.0.x86_64.rpm ./amazon-guardduty-
agent-1.1.0.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
x86_64/amazon-guardduty-agent-1.1.0.x86_64.sig ./amazon-guardduty-
agent-1.1.0.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
publickey.pem ./publickey.pem
```

Regione AWS	Nome Regione	AWS ID dell'account
eu-west-1	Europa (Irlanda)	694911143906
us-east-1	Stati Uniti orientali (Virginia settentrionale)	593207742271
us-west-2	US West (Oregon)	733349766148
eu-west-3	Europa (Parigi)	665651866788
us-east-2	Stati Uniti orientali (Ohio)	307168627858
eu-central-1	Europa (Francoforte)	323658145986
ap-northeast-2	Asia Pacifico (Seul)	914738172881
eu-north-1	Europa (Stoccolma)	591436053604
ap-east-1	Asia Pacifico (Hong Kong)	258348409381
me-south-1	Medio Oriente (Bahrein)	536382113932
eu-west-2	Europa (Londra)	892757235363
ap-northeast-1	Asia Pacifico (Tokyo)	533107202818
ap-southeast-1	Asia Pacifico (Singapore)	174946120834

ap-south-1	Asia Pacifico (Mumbai)	251508486986
ap-southeast-3	Asia Pacifico (Giacarta)	510637619217
sa-east-1	Sud America (San Paolo)	758426053663
ap-northeast-3	Asia Pacifico (Osaka-Lo cale)	273192626886
eu-south-1	Europa (Milano)	266869475730
af-south-1	Africa (Città del Capo)	197869348890
ap-southeast-2	Asia Pacifico (Sydney)	005257825471
me-central-1	Medio Oriente (Emirati Arabi Uniti)	000014521398
us-west-1	Stati Uniti occidentali (California settentrionale)	684579721401
ca-central-1	Canada (Centrale)	354763396469
ap-south-2	Asia Pacific (Hyderabad)	950823858135
eu-south-2	Europa (Spagna)	919611009337
eu-central-2	Europa (Zurigo)	529164026651
ap-southeast-4	Asia Pacifico (Melbourne)	251357961535
il-central-1	Israele (Tel Aviv)	870907303882

b. Importa la chiave pubblica nel database

```
gpg --import publickey.pem
```

gpg mostra che l'importazione è avvenuta con successo

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
```

```
gpg:               imported: 1  (RSA: 1)
```

c. Verifica la firma

```
gpg --verify amazon-guardduty-agent-1.1.0.x86_64.sig amazon-guardduty-
agent-1.1.0.x86_64.rpm
```

Se la verifica ha esito positivo, verrà visualizzato un messaggio simile al risultato riportato di seguito. È ora possibile procedere all'installazione del GuardDuty security agent utilizzando RPM.

Output di esempio:

```
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
```

Se la verifica fallisce, significa che la firma su RPM è stata potenzialmente manomessa. È necessario rimuovere la chiave pubblica dal database e ripetere il processo di verifica.

Esempio:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

d. Rimuovi la chiave pubblica dal database.

```
gpg --delete-keys AwsGuardDuty
```

2. Connect con SSH da Linux o macOS.
3. Installa il GuardDuty security agent utilizzando il seguente comando:

```
sudo rpm -ivh amazon-guardduty-agent-1.1.0.x86_64.rpm
```

4. Verifica se l'installazione dell' GuardDuty agente è integra. Per ulteriori informazioni sui passaggi, vedereConvalida dello stato di installazione del GuardDuty Security Agent.
5. (Facoltativo) rimuovete il GuardDuty security agent utilizzando il seguente comando:

```
sudo rpm -ev amazon-guardduty-agent
```

Errore di memoria esaurita

Se riscontri un `out-of-memory` errore durante l'installazione o l'aggiornamento manuale del GuardDuty Security Agent per Amazon EC2, consulta. Risoluzione dell'errore di esaurimento della memoria

Convalida dello stato di installazione del GuardDuty Security Agent

Per verificare se il GuardDuty Security Agent è integro

1. Connect con SSH da Linux o macOS.
2. Esegui il comando seguente per verificare lo stato del GuardDuty security agent:

```
sudo systemctl status amazon-guardduty-agent
```

Se desideri visualizzare i registri di installazione del Security Agent, sono disponibili in`/var/log/amzn-guardduty-agent/`.

Per visualizzare i log, fai. `sudo journalctl -u amazon-guardduty-agent`

Aggiornamento manuale del GuardDuty Security Agent

È possibile aggiornare il GuardDuty security agent utilizzando il comando Run. È possibile seguire gli stessi passaggi utilizzati per installare il GuardDuty security agent.

Disinstallazione manuale del Security Agent

Quando disabiliti il monitoraggio del runtime, GuardDuty non rimuove l'agente di sicurezza associato alla tua istanza Amazon EC2. Puoi disinstallare l'agente GuardDuty di sicurezza per l'istanza Amazon EC2 utilizzando uno dei due metodi seguenti.

Metodo 1: utilizzando il comando Esegui

Per disinstallare il GuardDuty security agent utilizzando il comando Run

1. È possibile disinstallare il GuardDuty security agent seguendo i passaggi specificati in AWS Systems Manager Esegui comando nella Guida per l'AWS Systems Manager utente. Utilizzate l'azione Disinstalla nei parametri per disinstallare il GuardDuty security agent.

   Nella sezione Target, assicurati che l'impatto riguardi solo le istanze Amazon EC2 da cui desideri disinstallare il security agent.

   Utilizza il seguente GuardDuty documento e distributore:

   - Nome del documento: `AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`
   - Distributore: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`
2. Dopo aver fornito tutti i dettagli, quando scegli Run, l'agente di sicurezza che ha distribuito sulle istanze Amazon EC2 di destinazione viene rimosso.

   Per rimuovere la configurazione degli endpoint Amazon VPC, devi disabilitare sia Runtime Monitoring che Amazon EKS Runtime Monitoring.

Metodo 2: utilizzando lo script RPM

Per disinstallare il GuardDuty security agent utilizzando rpm

1. Connect con SSH da Linux o macOS.
2. Il comando seguente disinstallerà il GuardDuty security agent dall'istanza Amazon EC2 a cui ti connetti:

   ```
   sudo rpm -e amazon-guardduty-agent
   ```

   Puoi anche controllare i log associati a questo comando.

Eliminare l'endpoint Amazon VPC

Se desideri disabilitare il Runtime Monitoring o disinstallare il GuardDuty security agent per il tuo account, puoi anche scegliere di eliminare l'endpoint Amazon VPC creato manualmente (). Creazione manuale di un endpoint Amazon VPC

Per eliminare l'endpoint Amazon VPC utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona l'endpoint che è stato creato manualmente al momento dell'attivazione del Runtime Monitoring.
4. Seleziona Actions (Operazioni), Delete VPC endpoints (Eliminazione di endpoint VPC).
5. Quando viene richiesta la conferma, immetti **`delete`**.
6. Scegli Elimina.

Per eliminare l'endpoint Amazon VPC utilizzando AWS CLI

- delete-vpc-endpoints (AWS Command Line Interface)
- VpcEndpoint Cmdlet Remove-EC2 (strumenti per Windows) PowerShell

Gestione dell'agente di sicurezza automatizzato per Fargate (solo Amazon ECS)

Configurazione dell' GuardDuty agente per un account autonomo

Attualmente, Runtime Monitoring supporta la gestione dell'agente di sicurezza per i cluster Amazon ECS (AWS Fargate) solo tramite. GuardDuty Non è disponibile alcun supporto per la gestione manuale del security agent sui cluster Amazon ECS.

Console

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione, scegli Runtime Monitoring.
3. Nella scheda Configurazione:

    a. Per gestire la configurazione automatizzata degli agenti per tutti i cluster Amazon ECS (a livello di account)

    Scegli Abilita nella sezione Configurazione automatica dell'agente per AWS Fargate (solo ECS). All'avvio di una nuova attività Fargate Amazon ECS, GuardDuty gestirà l'implementazione del security agent.

- Selezionare Salva.

b. Per gestire la configurazione automatizzata degli agenti escludendo alcuni cluster Amazon ECS (a livello di cluster)

i. Aggiungi un tag al cluster Amazon ECS per il quale desideri escludere tutte le attività. La coppia chiave-valore deve essere -. `GuardDutyManaged` `false`

ii. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "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:CreateTags",
```

```
                "ecs:DeleteTags"
            ],
            "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:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

iii. Nella scheda Configurazione, scegli Abilita nella sezione Configurazione automatica dell'agente.

> **Note**
>
> Aggiungi sempre il tag di esclusione al tuo cluster Amazon ECS prima di abilitare la gestione automatica degli GuardDuty agenti per il tuo account; in caso contrario, l'agente di sicurezza verrà distribuito in tutte le attività avviate all'interno del cluster Amazon ECS corrispondente.

Per i cluster Amazon ECS che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.

iv. Selezionare Salva.

c. Per gestire la configurazione automatizzata degli agenti includendo alcuni cluster Amazon ECS (a livello di cluster)

i. Aggiungi un tag a un cluster Amazon ECS per il quale desideri includere tutte le attività. La coppia chiave-valore deve essere -. `GuardDutyManaged` `true`

ii. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "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:CreateTags",
                "ecs:DeleteTags"
            ],
            "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:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

Configurazione GuardDuty dell'agente per un ambiente multi-account

In un ambiente con più account, solo l'account GuardDuty amministratore delegato può abilitare o disabilitare la configurazione automatica degli agenti per gli account dei membri e gestire la configurazione automatizzata degli agenti per i cluster Amazon ECS che appartengono agli account dei membri della loro organizzazione. Un account GuardDuty membro non può modificare questa configurazione. L'account GuardDuty amministratore delegato gestisce i propri account membro utilizzando AWS Organizations. Per ulteriori informazioni sugli ambienti con più account, vedere Gestione di più account in. GuardDuty

Abilitazione della configurazione automatizzata degli agenti per l'account amministratore delegato GuardDuty

Manage for all Amazon ECS clusters (account level)

Se hai scelto Abilita per tutti gli account per il monitoraggio del runtime, hai le seguenti opzioni:

- Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente. GuardDuty distribuirà e gestirà l'agente di sicurezza per tutte le attività di Amazon ECS che verranno lanciate.
- Scegli Configura gli account manualmente.

Se hai scelto Configura gli account manualmente nella sezione Runtime Monitoring, procedi come segue:

1. Scegli Configura gli account manualmente nella sezione Configurazione automatica degli agenti.
2. Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).

Selezionare Salva.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Aggiungi un tag a questo cluster Amazon ECS con la coppia chiave-valore come -. `GuardDutyManaged` `false`
2. Impedisci la modifica dei tag, tranne che da parte delle entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "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:CreateTags",
                "ecs:DeleteTags"
            ],
            "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:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
4. Nel pannello di navigazione, scegli Runtime Monitoring.

5.

> **Note**
>
> Aggiungi sempre il tag di esclusione ai tuoi cluster Amazon ECS prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario, il contenitore GuardDuty sidecar verrà collegato a tutti i contenitori delle attività di Amazon ECS che vengono lanciate.

   Nella scheda Configurazione, scegli Abilita nella configurazione automatizzata dell'agente.

   Per i cluster Amazon ECS che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.

6. Selezionare Salva.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Aggiungi un tag a un cluster Amazon ECS per il quale desideri includere tutte le attività. La coppia chiave-valore deve essere -. `GuardDutyManaged` `true`
2. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "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:CreateTags",
                "ecs:DeleteTags"
            ],
            "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:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Quando utilizzi tag di inclusione per i tuoi cluster Amazon ECS, non è necessario abilitare esplicitamente GuardDuty l'agente tramite la configurazione automatica degli agenti.

Attivazione automatica per tutti gli account dei membri

Manage for all Amazon ECS clusters (account level)

I passaggi seguenti presuppongono che tu abbia scelto Abilita per tutti gli account nella sezione Runtime Monitoring.

1. Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente. GuardDuty distribuirà e gestirà l'agente di sicurezza per tutte le attività di Amazon ECS che verranno lanciate.
2. Selezionare Salva.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Aggiungi un tag a questo cluster Amazon ECS con la coppia chiave-valore come -. `GuardDutyManaged` `false`
2. Impedisci la modifica dei tag, tranne che da parte delle entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${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:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
4. Nel riquadro di navigazione, scegli Runtime Monitoring.
5.

> **Note**
>
> Aggiungi sempre il tag di esclusione ai tuoi cluster Amazon ECS prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario, il contenitore GuardDuty sidecar verrà collegato a tutti i contenitori delle attività di Amazon ECS che vengono lanciate.

   Nella scheda Configurazione, scegli Modifica.
6. Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente

Per i cluster Amazon ECS che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.

7. Selezionare Salva.

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Indipendentemente da come scegli di abilitare il Runtime Monitoring, i seguenti passaggi ti aiuteranno a monitorare attività selettive di Amazon ECS Fargate per tutti gli account membri della tua organizzazione.

1. Non abilitare alcuna configurazione nella sezione Configurazione automatica dell'agente. Mantieni la configurazione di Runtime Monitoring uguale a quella selezionata nel passaggio precedente.
2. Selezionare Salva.
3. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "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:CreateTags",
                "ecs:DeleteTags"
            ],
            "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:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
```

```
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Quando utilizzi tag di inclusione per i tuoi cluster Amazon ECS, non è necessario abilitare esplicitamente la gestione automatica degli GuardDuty agenti.

Abilitazione della configurazione automatizzata degli agenti per gli account dei membri attivi esistenti

Manage for all Amazon ECS clusters (account level)

1. Nella pagina Runtime Monitoring, nella scheda Configurazione, è possibile visualizzare lo stato corrente della configurazione automatizzata dell'agente.
2. Nel riquadro di configurazione dell'agente automatizzato, nella sezione Account membri attivi, scegli Azioni.
3. Da Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
4. Scegli Conferma.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Aggiungi un tag a questo cluster Amazon ECS con la coppia chiave-valore come -. `GuardDutyManaged` `false`
2. Impedisci la modifica dei tag, tranne che da parte delle entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
```

```
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${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:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Apri la GuardDuty console all'[indirizzo https://console.aws.amazon.com/guardduty/](https://console.aws.amazon.com/guardduty/).
4. Nel riquadro di navigazione, scegli Runtime Monitoring.
5.

> **Note**
>
> Aggiungi sempre il tag di esclusione ai tuoi cluster Amazon ECS prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario, il contenitore GuardDuty sidecar verrà collegato a tutti i contenitori delle attività di Amazon ECS che vengono lanciate.

   Nella scheda Configurazione, nella sezione Configurazione automatizzata dell'agente, in Account membri attivi, scegli Azioni.
6. Da Operazioni, scegli Abilita per tutti gli account membri attivi.

   Per i cluster Amazon ECS che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.
7. Scegli Conferma.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Aggiungi un tag a un cluster Amazon ECS per il quale desideri includere tutte le attività. La coppia chiave-valore deve essere -. `GuardDutyManaged` `true`
2. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "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:CreateTags",
                "ecs:DeleteTags"
            ],
            "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:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Quando utilizzi tag di inclusione per i tuoi cluster Amazon ECS, non è necessario abilitare esplicitamente la configurazione degli agenti automatizzati.

Abilita automaticamente la configurazione automatizzata degli agenti per i nuovi membri

Manage for all Amazon ECS clusters (account level)

1. Nella pagina Runtime Monitoring, scegli Modifica per aggiornare la configurazione esistente.
2. Nella sezione Configurazione automatizzata dell'agente, seleziona Abilita automaticamente per nuovi account membro.
3. Selezionare Salva.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Aggiungi un tag a questo cluster Amazon ECS con la coppia chiave-valore come -. `GuardDutyManaged` `false`
2. Impedisci la modifica dei tag, tranne che da parte delle entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "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:CreateTags",
                "ecs:DeleteTags"
            ],
            "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:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
```

```
        }
    ]
}
```

3. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
4. Nel riquadro di navigazione, scegli Runtime Monitoring.
5.

> **Note**
>
> Aggiungi sempre il tag di esclusione ai tuoi cluster Amazon ECS prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario, il contenitore GuardDuty sidecar verrà collegato a tutti i contenitori delle attività di Amazon ECS che vengono lanciate.

   Nella scheda Configurazione, seleziona Abilita automaticamente gli account dei nuovi membri nella sezione Configurazione automatica degli agenti.

   Per i cluster Amazon ECS che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.
6. Selezionare Salva.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Aggiungi un tag a un cluster Amazon ECS per il quale desideri includere tutte le attività. La coppia chiave-valore deve essere -. `GuardDutyManaged` `true`
2. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
```

```
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${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:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Quando utilizzi tag di inclusione per i tuoi cluster Amazon ECS, non è necessario abilitare esplicitamente la configurazione degli agenti automatizzati.

Abilitazione selettiva della configurazione automatizzata degli agenti per gli account dei membri attivi

Manage for all Amazon ECS (account level)

1. Nella pagina Account, selezionare gli account per i quali si desidera abilitare la configurazione dell'agente Runtime Monitoring-Automated (ECS-Fargate). È possibile selezionare più account. Assicurati che gli account selezionati in questo passaggio siano già abilitati con Runtime Monitoring.
2. Da Modifica piani di protezione, scegli l'opzione appropriata per abilitare la configurazione automatica degli agenti di monitoraggio del runtime (ECS-Fargate).
3. Scegli Conferma.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Aggiungi un tag a questo cluster Amazon ECS con la coppia chiave-valore come -. `GuardDutyManaged` `false`
2. Impedisci la modifica dei tag, tranne che da parte delle entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "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:CreateTags",
                "ecs:DeleteTags"
            ],
            "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:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Apri la GuardDuty console all'[indirizzo https://console.aws.amazon.com/guardduty/](https://console.aws.amazon.com/guardduty/).
4. Nel riquadro di navigazione, scegli Runtime Monitoring.

5.
> **Note**
>
> Aggiungi sempre il tag di esclusione ai tuoi cluster Amazon ECS prima di abilitare la gestione automatica degli GuardDuty agenti per il tuo account; in caso contrario, il contenitore GuardDuty sidecar verrà collegato a tutti i contenitori delle attività di Amazon ECS che vengono lanciate.

   Nella pagina Account, selezionare gli account per i quali si desidera abilitare la configurazione dell'agente Runtime Monitoring-Automated (ECS-Fargate). È possibile selezionare più account. Assicurati che gli account selezionati in questo passaggio siano già abilitati con Runtime Monitoring.

   Per i cluster Amazon ECS che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.

6. Da Modifica piani di protezione, scegli l'opzione appropriata per abilitare la configurazione automatica degli agenti di monitoraggio del runtime (ECS-Fargate).
7. Selezionare Salva.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Assicurati di non abilitare la configurazione automatizzata degli agenti (o la configurazione degli agenti automatizzati di Runtime Monitoring-ECS-Fargate) per gli account selezionati che hanno i cluster Amazon ECS che desideri monitorare.
2. Aggiungi un tag a un cluster Amazon ECS per il quale desideri includere tutte le attività. La coppia chiave-valore deve essere -. `GuardDutyManaged` `true`
3. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
```

```
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${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:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Quando utilizzi tag di inclusione per i tuoi cluster Amazon ECS, non è necessario abilitare esplicitamente la configurazione degli agenti automatizzati.

Gestione automatica dell'agente di sicurezza per i cluster Amazon EKS

Configurazione dell'agente automatizzato per un account indipendente

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione, scegli Runtime Monitoring.
3. Nella scheda Configurazione, scegli Abilita per abilitare la configurazione automatica degli agenti per il tuo account.

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (Monitorare tutti i cluster EKS)	1. Scegli Abilita nella sezione Configurazione automatica dell'agente. GuardDuty gestirà l'implementazione e gli aggiornamenti del security agent per tutti i cluster EKS esistenti e potenzialmente nuovi nel tuo account. 2. Selezionare Salva.

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite il tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti. Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent non è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave `GuardDutyManaged` e il valore corrispondente `false`. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *`ec2: CreateTags`* con. `eks:TagResource` • Sostituisci *`ec2: DeleteTags`* con. `eks:UntagResource` • Sostituisci *`access-project`* con `GuardDutyManaged` • Sostituisci *`123456789012`* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-`

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
	admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"] 3. Apri la console all'indirizzo https://console.aws.amazon.com/guardduty/ GuardDuty . 4. Nel riquadro di navigazione, scegli Runtime Monitoring. **Note** Aggiungi sempre il tag di esclusione ai tuoi cluster EKS prima di abilitare la gestione automatica degli GuardDuty agenti per il tuo account; in caso contrario, l'agente GuardDuty di sicurezza verrà distribuito su tutti i cluster EKS del tuo account. 5. Nella scheda Configurazione, scegli Abilita nella sezione Gestione degli agenti. GuardDuty Per i cluster EKS che non sono stati esclusi dal monitoraggio, GuardDuty gestirà la distribuzione e gli aggiornamenti del GuardDuty security agent. 6. Selezionare Salva. Per escludere un cluster EKS dal monitoraggio dopo che il GuardDuty security agent è già stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave `GuardDutyManaged` e il valore corrispondente `false`.

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
	Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. Dopo questo passaggio, non GuardDuty aggiorner à il security agent per questo cluster. Tuttavia, il security agent rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo cluster EKS. Ciò potrebbe influire sulle statistiche di utilizzo. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizat ions . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con. `eks:TagRe source` • Sostituisci *ec2: DeleteTags* con. `eks:Untag Resource` • Sostituisci *access-project* con `GuardDuty Managed` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::12 3456789012:role/org-admins/iam- admin", "arn:aws:iam::123456789012: role/org-admins/iam-admin", "arn:aws:`

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
	<pre>iam::123456789012:role/org-admins/ia m-admin"]</pre> 3. È necessario rimuovere l'agente di sicurezza implementato dal cluster EKS per interrompere la ricezione degli eventi di runtime dal cluster in questione. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Pulizia delle risorse del Security Agent GuardDuty .

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
Monitorare cluster EKS selettivi utilizzando i tag di inclusione	1. Assicurati di scegliere Disabilita nella sezione Configurazione automatica dell'agente. Mantieni abilitato il monitoraggio del runtime. 2. Seleziona Salva 3. Aggiungi un tag a questo cluster EKS con la chiave `GuardDutyManaged` e il valore corrispondente `true`. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. GuardDuty gestirà l'implementazione e gli aggiornamenti del security agent per i cluster EKS selettivi che desideri monitorare. 4. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2:* con. CreateTags `eks:TagResource` • Sostituisci *ec2: DeleteTags* con. `eks:UntagResource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` :

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
	`"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"]`
Gestire l'agente manualmente	1. Assicurati di scegliere Disabilita nella sezione Configurazione automatica dell'agente. Mantieni abilitato il monitoraggio del runtime. 2. Selezionare Salva. 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Configurazione dell'agente automatizzato per ambienti con più account

In ambienti con più account, solo l'account GuardDuty amministratore delegato può abilitare o disabilitare la configurazione automatizzata degli agenti per gli account dei membri e gestire l'agente automatizzato per i cluster EKS appartenenti agli account membro dell'organizzazione. GuardDuty Gli account dei membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce gli account dei membri utilizzando AWS Organizations. Per ulteriori informazioni sugli ambienti multi-account, consulta Gestione di più account.

Configurazione della configurazione automatizzata dell'agente per l'account amministratore delegato GuardDuty

Approccio preferito per la gestione del Security Agent GuardDuty	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (Monitorare tutti i cluster EKS)	Se hai scelto Abilita per tutti gli account nella sezione Runtime Monitoring, hai le seguenti opzioni: • Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente. GuardDuty implementerà e gestirà l'agente di sicurezza per tutti i cluster EKS che appartengono all'account GuardDuty amministratore delegato e anche per tutti i cluster EKS che appartengono a tutti gli account membro esistenti e potenzial mente nuovi dell'organizzazione. • Scegli Configura gli account manualmente. Se hai scelto Configura gli account manualmente nella sezione Runtime Monitoring, procedi come segue: 1. Scegli Configura gli account manualmente nella sezione Configura zione automatica degli agenti. 2. Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account). Selezionare Salva.
Monitorare tutti i cluster EKS escludendone alcuni (tramite i tag di esclusion e)	Scegli lo scenario più adatto a te tra le procedure seguenti. Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent non è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave `GuardDuty Managed` e il valore corrispondente `false`.

Approccio preferito per la gestione del Security Agent GuardDuty	Fasi
	Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con. `eks:TagResource` • Sostituisci *ec2: DeleteTags* con. `eks:UntagResource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `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. Apri la console all'indirizzo https://console.aws.amazon.com/guardduty/ GuardDuty . 4. Nel riquadro di navigazione, scegli Runtime Monitoring. **Note** Aggiungi sempre il tag di esclusione ai tuoi cluster EKS prima di abilitare la gestione automatica degli GuardDuty agenti per il tuo account; in caso contrario, l'agente

Approccio preferito per la gestione del Security Agent GuardDuty	Fasi
	GuardDuty di sicurezza verrà distribuito su tutti i cluster EKS del tuo account. 5. Nella scheda Configurazione, scegli Abilita nella sezione Gestione degli agenti. GuardDuty Per i cluster EKS che non sono stati esclusi dal monitorag gio, GuardDuty gestirà la distribuzione e gli aggiornamenti del GuardDuty security agent. 6. Selezionare Salva. Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave `GuardDuty Managed` e il valore corrispondente `false`. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *`ec2: CreateTags`* con. `eks:TagResource` • Sostituisci *`ec2: DeleteTags`* con. `eks:UntagResource` • Sostituisci *`access-project`* con `GuardDutyManaged` • Sostituisci *`123456789012`* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` :

Approccio preferito per la gestione del Security Agent GuardDuty	Fasi
	<pre>"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"]</pre> 3. Se l'agente automatizzato era abilitato per questo cluster EKS, dopo questo passaggio non GuardDuty aggiornerà il security agent per questo cluster. Tuttavia, il security agent rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo cluster EKS. Ciò potrebbe influire sulle statistiche di utilizzo. È necessario rimuovere l'agente di sicurezza implementato dal cluster EKS per interrompere la ricezione degli eventi di runtime dal cluster in questione. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Pulizia delle risorse del Security Agent GuardDuty 4. Se stavi gestendo manualmente il GuardDuty security agent per questo cluster EKS, vediPulizia delle risorse del Security Agent GuardDuty .

Approccio preferito per la gestione del Security Agent GuardDuty	Fasi
Monitorare cluster EKS selettivi utilizzando i tag di inclusione	Indipendentemente dal modo in cui avete scelto di abilitare il Runtime Monitoring, i seguenti passaggi vi aiuteranno a monitorare i cluster EKS selettivi nel vostro account: 1. Assicurati di scegliere Disattiva per l'account GuardDuty amministratore delegato (questo account) nella sezione Configurazione automatica dell'agente. Mantieni la configura zione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. 2. Selezionare Salva. 3. Aggiungi un tag al cluster EKS con la chiave `GuardDuty Managed` e il valore corrispondente `true`. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per i cluster EKS selettivi che si desidera monitorare. 4. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2:* con. CreateTags `eks:TagResource` • Sostituisci *ec2: DeleteTags* con. `eks:UntagResource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` :

Approccio preferito per la gestione del Security Agent GuardDuty	Fasi
	`"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"]`
Gestisci manualmente l'agente di sicurezza GuardDuty	Indipendentemente dal modo in cui avete scelto di abilitare il Runtime Monitoring, potete gestire manualmente il security agent per i cluster EKS. 1. Assicurati di scegliere Disabilita per l'account GuardDuty amministratore delegato (questo account) nella sezione Configurazione automatica dell'agente. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. 2. Selezionare Salva. 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Abilita automaticamente l'agente automatizzato per tutti gli account dei membri

> **Note**
>
> L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty	Questo argomento riguarda l'abilitazione del monitoraggio del runtime per tutti gli account membri e, pertanto, i passaggi seguenti

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
(Monitorare tutti i cluster EKS)	presuppongono che sia necessario aver scelto Abilita per tutti gli account nella sezione Runtime Monitoring. 1. Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente. GuardDuty implementerà e gestirà l'agente di sicurezza per tutti i cluster EKS che appartengono all'account GuardDuty amministratore delegato e anche per tutti i cluster EKS che appartengono a tutti gli account membro esistenti e potenzialmente nuovi dell'organizzazione. 2. Selezionare Salva.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite i tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti. Per escludere un cluster EKS dal monitoraggio quando l'agente GuardDuty di sicurezza non è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave `GuardDuty Managed` e il valore corrispondente `false`. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con. `eks:TagResource` • Sostituisci *ec2: DeleteTags* con. `eks:UntagResource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `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. Apri la console all'indirizzo https://console.aws.amazon.com/guardduty/ GuardDuty . 4. Nel riquadro di navigazione, scegli Runtime Monitoring.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	> **Note** > Aggiungi sempre il tag di esclusione ai tuoi cluster EKS prima di abilitare Automated Agent per il tuo account; in caso contrario, l'agente di GuardDuty sicurezza verrà distribuito su tutti i cluster EKS del tuo account. 5. Nella scheda Configurazione, scegli Modifica nella sezione Configurazione di Runtime Monitoring. 6. Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente. Per i cluster EKS che non sono stati esclusi dal monitoraggio, GuardDuty gestirà la distribuzione e gli aggiornamenti del GuardDuty security agent. 7. Selezionare Salva. Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave `GuardDuty Managed` e il valore corrispondente `false`. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. 2. Se la configurazione automatizzata dell'agente era abilitata per questo cluster EKS, dopo questo passaggio non GuardDuty aggiornerà l'agente di sicurezza per questo cluster. Tuttavia, l'agente di sicurezza rimarrà distribuito e GuardDuty continuer à a ricevere gli eventi di runtime da questo cluster EKS. Ciò potrebbe influire sulle statistiche di utilizzo.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	È necessario rimuovere l'agente di sicurezza implementato dal cluster EKS per interrompere la ricezione degli eventi di runtime dal cluster in questione. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Pulizia delle risorse del Security Agent GuardDuty 3. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con. `eks:TagResource` • Sostituisci *ec2: DeleteTags* con. `eks:UntagResource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `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"]` 4. Se stavi gestendo manualmente il GuardDuty security agent per questo cluster EKS, vedi. Pulizia delle risorse del Security Agent GuardDuty

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitorare cluster EKS selettivi utilizzando i tag di inclusione	Indipendentemente dal modo in cui avete scelto di abilitare il Runtime Monitoring, i seguenti passaggi vi aiuteranno a monitorare i cluster EKS selettivi per tutti gli account membri della vostra organizzazione: 1. Non abilitate alcuna configurazione nella sezione Configurazione automatica dell'agente. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedent e. 2. Selezionare Salva. 3. Aggiungi un tag al cluster EKS con la chiave `GuardDuty Managed` e il valore corrispondente `true`. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per i cluster EKS selettivi che si desidera monitorare. 4. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2:* con. CreateTags `eks:TagResource` • Sostituisci *ec2: DeleteTags* con. `eks:UntagResource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` :

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	`"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"]`
Gestisci manualmente l'agente di sicurezza GuardDuty	Indipendentemente dal modo in cui avete scelto di abilitare il Runtime Monitoring, potete gestire manualmente il security agent per i cluster EKS. 1. Non abilitate alcuna configurazione nella sezione Configurazione automatizzata dell'agente. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. 2. Selezionare Salva. 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Attivazione dell'agente automatizzato per tutti gli account dei membri attivi esistenti

> **Note**
>
> L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Per gestire il GuardDuty Security Agent per gli account dei membri attivi esistenti nell'organizzazione

- GuardDuty Per ricevere gli eventi di runtime dai cluster EKS che appartengono agli account dei membri attivi esistenti nell'organizzazione, è necessario scegliere un approccio preferito per gestire l'agente di GuardDuty sicurezza per questi cluster EKS. Per ulteriori informazioni su ognuno di questi approcci, consulta Approcci per gestire l'agente di sicurezza GuardDuty.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (Monitorare tutti i cluster EKS)	Per monitorare tutti i cluster EKS per tutti gli account membri attivi esistenti 1. Nella pagina Runtime Monitoring, nella scheda Configurazione, è possibile visualizzare lo stato corrente della configurazione automatizzata dell'agente. 2. Nel riquadro di configurazione dell'agente automatizzato, nella sezione Account membri attivi, scegli Azioni. 3. Da Operazioni, scegli Abilita per tutti gli account membri attivi esistenti. 4. Scegli Conferma.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite il tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti. Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent non è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave `GuardDutyManaged` e il valore corrispondente `false`. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *`ec2: CreateTags`* con. `eks:TagResource` • Sostituisci *`ec2: DeleteTags`* con. `eks:UntagResource` • Sostituisci *`access-project`* con `GuardDutyManaged` • Sostituisci *`123456789012`* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-`

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
	admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
	3. Apri la console all'indirizzo https://console.aws.amazon.com/guardduty/ GuardDuty . 4. Nel riquadro di navigazione, scegli Runtime Monitoring. **Note** Aggiungi sempre il tag di esclusione ai tuoi cluster EKS prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account. 5. Nella scheda Configurazione, nel riquadro Configurazione automatizzata dell'agente, in Account membri attivi, scegli Azioni. 6. Da Operazioni, scegli Abilita per tutti gli account membri attivi. 7. Scegli Conferma. Per escludere un cluster EKS dal monitoraggio dopo che il GuardDuty security agent è già stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave `GuardDutyManaged` e il valore corrispondente `false`.

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
	Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. Dopo questo passaggio, non GuardDuty aggiorner à il security agent per questo cluster. Tuttavia, il security agent rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo cluster EKS. Ciò potrebbe influire sulle statistiche di utilizzo. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizat ions . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con. `eks:TagRe source` • Sostituisci *ec2: DeleteTags* con. `eks:Untag Resource` • Sostituisci *access-project* con `GuardDuty Managed` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::12 3456789012:role/org-admins/iam- admin", "arn:aws:iam::123456789012: role/org-admins/iam-admin", "arn:aws:`

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
	iam::123456789012:role/org-admins/iam-admin"] 3. Indipendentemente dal modo in cui gestisci il security agent (tramite GuardDuty o manualmente), per interrompere la ricezione degli eventi di runtime da questo cluster, devi rimuovere l'agente di sicurezza distribuito da questo cluster EKS. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Pulizia delle risorse del Security Agent GuardDuty .

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
Monitorare cluster EKS selettivi utilizzando i tag di inclusione	1. Nella pagina Account, dopo aver abilitato Runtime Monitoring, non attivate Runtime Monitoring - Configurazione automatica dell'agente. 2. Aggiungi un tag al cluster EKS che appartiene all'account selezionato che desideri monitorare. La coppia chiave-valore del tag deve essere `GuardDutyManaged -true`. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per i cluster EKS selettivi che si desidera monitorare. 3. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2:* con. CreateTags `eks:TagResource` • Sostituisci *ec2: DeleteTags* con. `eks:UntagResource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` :

Approccio preferito per la gestione GuardDuty degli agenti di sicurezza	Fasi
	`"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"]`
Gestisci manualmente l'agente di sicurezza GuardDuty	1. Assicurati di non scegliere Abilita nella sezione Configurazione automatica dell'agente. Mantieni abilitato il monitoraggio del runtime. 2. Selezionare Salva. 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Abilita automaticamente la configurazione automatica degli agenti per i nuovi membri

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (Monitorare tutti i cluster EKS)	1. Nella pagina Runtime Monitoring, scegli Modifica per aggiornare la configurazione esistente. 2. Nella sezione Configurazione automatizzata dell'agente, seleziona Abilita automaticamente per nuovi account membro. 3. Selezionare Salva.
Monitorare tutti i cluster EKS escludendone alcuni (tramite i tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent non è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave `GuardDutyManaged` e il valore corrispondente `false`. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con. `eks:TagResource` • Sostituisci *ec2: DeleteTags* con. `eks:UntagResource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `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"]`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	3. Apri la console all'indirizzo https://console.aws.amazon.com/guardduty/ GuardDuty . 4. Nel riquadro di navigazione, scegli Runtime Monitoring. **Note** Aggiungi sempre il tag di esclusione ai tuoi cluster EKS prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account. 5. Nella scheda Configurazione, seleziona Abilita automaticamente gli account dei nuovi membri nella sezione Gestione degli GuardDuty agenti. Per i cluster EKS che non sono stati esclusi dal monitoraggio, GuardDuty gestirà la distribuzione e gli aggiornamenti del GuardDuty security agent. 6. Selezionare Salva. Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent è stato distribuito su questo cluster 1. Indipendentemente dal fatto che gestiate il GuardDuty security agent tramite GuardDuty o manualmente, aggiungete un tag a questo cluster EKS con la chiave as `GuardDutyManaged` e il relativo valore. `false` Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Se l'agente automatizzato era abilitato per questo cluster EKS, dopo questo passaggio non GuardDuty aggiornerà l'agente di sicurezza per questo cluster. Tuttavia, l'agente di sicurezza rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo cluster EKS. Ciò potrebbe influire sulle statistic he di utilizzo. È necessario rimuovere l'agente di sicurezza implement ato dal cluster EKS per interrompere la ricezione degli eventi di runtime dal cluster in questione. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Pulizia delle risorse del Security Agent GuardDuty 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizza ti nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con. `eks:TagRe source` • Sostituisci *ec2: DeleteTags* con. `eks:Untag Resource` • Sostituisci *access-project* con `GuardDuty Managed` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::12 3456789012:role/org-admins/iam-admin`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
	3. Se stavi gestendo manualmente il GuardDuty security agent per questo cluster EKS, vedi. Pulizia delle risorse del Security Agent GuardDuty

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitorare cluster EKS selettivi utilizzando i tag di inclusione	Indipendentemente dal modo in cui avete scelto di abilitare il Runtime Monitoring, i seguenti passaggi vi aiuterann o a monitorare i cluster EKS selettivi per i nuovi account membro della vostra organizzazione. 1. Assicurati di deselezionare Abilita automaticamente per nuovi account membro nella sezione Configurazione automatica degli agenti. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. 2. Selezionare Salva. 3. Aggiungi un tag al cluster EKS con la chiave `GuardDutyManaged` e il valore corrispondente `true`. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. GuardDuty gestirà la distribuzione e gli aggiornam enti del security agent per i cluster EKS selettivi che si desidera monitorare. 4. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizza ti nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *`ec2:`* con. CreateTags `eks:TagRe source` • Sostituisci *`ec2: DeleteTags`* con. `eks:Untag Resource` • Sostituisci *`access-project`* con `GuardDuty Managed`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	• Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `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"]`
Gestisci manualmente l'agente di sicurezza GuardDuty	Indipendentemente dal modo in cui avete scelto di abilitare il Runtime Monitoring, potete gestire manualmente il security agent per i cluster EKS. 1. Assicurati di deselezionare la casella di controllo Abilita automaticamente gli account dei nuovi membri nella sezione Configurazione automatica degli agenti. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. 2. Selezionare Salva. 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Configurazione selettiva dell'agente automatizzato per gli account dei membri attivi

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (Monitorare tutti i cluster EKS)	1. Nella pagina Account, seleziona gli account per i quali desideri abilitare la configurazione automatica degli agenti. Puoi selezionare più di un account alla volta. Assicurati che il monitoraggio del runtime EKS sia già abilitato per gli account selezionati in questa fase. 2. Da Modifica piani di protezione, scegli l'opzione appropriata per abilitare Runtime Monitoring - Configurazione automatica degli agenti. 3. Scegli Conferma.
Monitorare tutti i cluster EKS escludendone alcuni (tramite i tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti. Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent non è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave `GuardDuty Managed` e il valore corrispondente `false`. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *`ec2: CreateTags`* con. `eks:TagResource` • Sostituisci *`ec2: DeleteTags`* con. `eks:UntagResource` • Sostituisci *`access-project`* con `GuardDutyManaged` • Sostituisci *`123456789012`* con l' Account AWS ID dell'entità affidabile.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi

Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `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. Apri la console all'indirizzo https://console.aws.amazon.com/guardduty/ GuardDuty .

> **Note**
>
> Aggiungi sempre il tag di esclusione ai tuoi cluster EKS prima di abilitare la configurazione automatizzata dell'agente per il tuo account; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account.

4. Nella pagina Account, seleziona l'account per il quale desideri abilitare Gestisci automaticamente l'agente. Puoi selezionare più di un account alla volta.
5. Da Modifica piani di protezione, scegliete l'opzione appropriata per abilitare la configurazione automatica dell'agente di monitoraggio del runtime per l'account selezionato.

   Per i cluster EKS che non sono stati esclusi dal monitoraggio, GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent. GuardDuty
6. Selezionare Salva.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Per escludere un cluster EKS dal monitoraggio quando il GuardDuty security agent è stato distribuito su questo cluster 1. Aggiungi un tag a questo cluster EKS con la chiave `GuardDuty Managed` e il valore corrispondente `false`. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. Se in precedenza era stata abilitata la configurazione dell'agen te automatizzato per questo cluster EKS, dopo questo passaggio non GuardDuty aggiornerà il security agent per questo cluster. Tuttavia, l'agente di sicurezza rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo cluster EKS. Ciò potrebbe influire sulle statistiche di utilizzo. È necessario rimuovere l'agente di sicurezza implementato dal cluster EKS per interrompere la ricezione degli eventi di runtime dal cluster in questione. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Pulizia delle risorse del Security Agent GuardDuty 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *`ec2: CreateTags`* con. `eks:TagResource` • Sostituisci *`ec2: DeleteTags`* con. `eks:UntagResource` • Sostituisci *`access-project`* con `GuardDutyManaged` • Sostituisci *`123456789012`* con l' Account AWS ID dell'entità affidabile.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `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. Se stavi gestendo manualmente il GuardDuty security agent per questo cluster EKS, devi rimuoverlo. Per ulteriori informazioni, consulta Pulizia delle risorse del Security Agent GuardDuty .

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitorare cluster EKS selettivi utilizzando i tag di inclusione	Indipendentemente dal modo in cui avete scelto di abilitare il Runtime Monitoring, i seguenti passaggi vi aiuteranno a monitorare i cluster EKS selettivi che appartengono agli account selezionati: 1. Assicuratevi di non abilitare la configurazione automatica degli agenti di Runtime Monitoring-Automated per gli account selezionati che dispongono dei cluster EKS che desiderate monitorare. 2. Aggiungi un tag al cluster EKS con la chiave `GuardDuty Managed` e il valore corrispondente `true`. Per ulteriori informazioni sull'assegnazione di tag al cluster Amazon EKS, consulta Utilizzo di tag tramite la console nella Guida per l'utente di Amazon EKS. Dopo aver aggiunto il tag, GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per i cluster EKS selettivi che desideri monitorare. 3. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *`ec2:`* con. CreateTags `eks:TagResource` • Sostituisci *`ec2: DeleteTags`* con. `eks:UntagResource` • Sostituisci *`access-project`* con `GuardDutyManaged` • Sostituisci *`123456789012`* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` :

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	`"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"]`
Gestisci manualmente l'agente di sicurezza GuardDuty	1. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. Assicurati di non abilitare Runtime Monitoring - Configurazione automatica degli agenti per nessuno degli account selezionati. 2. Scegli Conferma. 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS

Questa sezione descrive come gestire il tuo agente aggiuntivo Amazon EKS (GuardDuty agente) dopo aver abilitato il Runtime Monitoring. Per utilizzare Runtime Monitoring, devi abilitare Runtime Monitoring e configurare il componente aggiuntivo Amazon EKS,`aws-guardduty-agent`. L'esecuzione di una sola di queste due fasi non aiuterà a GuardDuty rilevare potenziali minacce o a generare risultati.

Prerequisiti per l'implementazione del Security Agent GuardDuty

Questa sezione descrive i prerequisiti per la distribuzione manuale del GuardDuty Security Agent per i cluster EKS. Prima di procedere, assicuratevi di aver già configurato il Runtime Monitoring per i vostri account. L'agente GuardDuty di sicurezza (componente aggiuntivo EKS) non funzionerà se non configuri il Runtime Monitoring. Per ulteriori informazioni, consulta Abilitazione del monitoraggio del GuardDuty runtime. Una volta completate la fasi seguenti, consulta GuardDuty Implementazione di un agente di sicurezza.

Scegli il metodo di accesso che preferisci per creare un endpoint Amazon VPC.

Console

Creare un endpoint VPC

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Dal riquadro di navigazione, in Cloud privato virtuale, scegli Endpoint.
3. Scegliere Create Endpoint (Crea endpoint).
4. Nella pagina Crea endpoint per Categoria servizio, scegli Altri servizi endpoint.
5. Per Nome servizio, inserisci **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**.

   Assicurati di sostituire *`us-east-1`* con la regione corretta. Questa deve essere la stessa regione del cluster EKS che appartiene al tuo Account AWS ID.
6. Scegli Verifica del servizio.
7. Dopo aver verificato correttamente il nome del servizio, scegli il VPC in cui risiede il cluster. Aggiungi la policy seguente per limitare l'utilizzo degli endpoint VPC solo all'account specificato. Con la `Condition` dell'organizzazione fornita sotto a questa policy, puoi aggiornare la policy seguente per limitare l'accesso all'endpoint. Per fornire il supporto degli endpoint VPC a ID account specifici della tua organizzazione, consulta Organization condition to restrict access to your endpoint.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
```

```
 ]
}
```

L'ID account di `aws:PrincipalAccount` deve corrispondere all'account contenente il VPC e l'endpoint VPC. L'elenco seguente mostra come condividere l'endpoint VPC con altri ID Account AWS :

Condizione dell'organizzazione per limitare l'accesso all'endpoint

- Per specificare più account per accedere all'endpoint VPC, sostituisci `"aws:PrincipalAccount": "111122223333"` con quanto segue:

```
"aws:PrincipalAccount": [
          "666666666666",
          "555555555555"
    ]
```

- Per consentire a tutti i membri di un'organizzazione di accedere all'endpoint VPC, sostituisci `"aws:PrincipalAccount": "111122223333"` con quanto segue:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- Per limitare l'accesso a una risorsa da parte di un ID organizzazione, aggiungi il tuo `ResourceOrgID` alla policy.

  Per ulteriori informazioni, consulta ResourceOrgID.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. In Impostazioni aggiuntive, scegli Abilita nome DNS.
9. In Sottoreti, scegli le sottoreti in cui risiede il cluster.
10. In Gruppi di sicurezza, scegli un gruppo di sicurezza con la porta 443 in ingresso abilitata dal tuo VPC (o dal cluster EKS). Se non disponi già di un gruppo di sicurezza con una porta 443 in ingresso abilitata, Crea un gruppo di sicurezza.

    Se si verifica un problema durante la limitazione delle autorizzazioni in ingresso al tuo VPC (o cluster), fornisci il supporto alla porta 443 in ingresso da qualsiasi indirizzo IP (`0.0.0.0/0`).

API/CLI

- CreateVpcEndpointInvoca.
- Utilizza i seguenti valori per i parametri:
  - Per Nome servizio, inserisci **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**.

    Assicurati di sostituire *`us-east-1`* con la regione corretta. Deve essere la stessa regione del cluster EKS che appartiene al tuo Account AWS ID.
  - Per DNSOptions, abilita l'opzione DNS privato impostandola su `true`.
- Per AWS Command Line Interface, vedi create-vpc-endpoint.

Configurazione GuardDuty dei parametri dell'agente di sicurezza (componente aggiuntivo) per Amazon EKS

Puoi configurare parametri specifici del tuo agente di GuardDuty sicurezza per Amazon EKS. Questo supporto è disponibile per la versione 1.5.0 e successive del GuardDuty Security Agent. Per informazioni sulle ultime versioni dei componenti aggiuntivi, consulta. GuardDuty agente di sicurezza per cluster Amazon EKS

Perché devo aggiornare lo schema di configurazione del Security Agent

> Lo schema di configurazione per l'agente GuardDuty di sicurezza è lo stesso per tutti i contenitori all'interno dei cluster Amazon EKS. Quando i valori predefiniti non sono in linea con i carichi di lavoro associati e le dimensioni dell'istanza, prendi in considerazione la configurazione delle impostazioni della CPU, delle impostazioni della memoria e delle impostazioni. `PriorityClass` `dnsPolicy` Indipendentemente da come gestisci l' GuardDuty agente per i tuoi cluster Amazon EKS, puoi configurare o aggiornare la configurazione esistente di questi parametri.

Comportamento di configurazione automatizzato degli agenti con parametri configurati

Quando GuardDuty gestisce il security agent (componente aggiuntivo EKS) per conto dell'utente, aggiorna il componente aggiuntivo, se necessario. GuardDuty imposterà il valore dei parametri configurabili su un valore predefinito. Tuttavia, è ancora possibile aggiornare i parametri al valore desiderato. Se ciò causa un conflitto, l'opzione predefinita per ResolveConflicts è. `None`

Parametri e valori configurabili

Per informazioni sui passaggi per configurare i parametri del componente aggiuntivo, consulta:

- GuardDuty Implementazione di un agente di sicurezza o
- Aggiornamento manuale del security agent

Le tabelle seguenti forniscono gli intervalli e i valori che puoi utilizzare per distribuire manualmente il componente aggiuntivo Amazon EKS o aggiornare le impostazioni del componente aggiuntivo esistenti.

Impostazioni della CPU

Parametri	Valore predefinito	Intervallo configurabile
Richieste	200 m	Tra 200 m e 10000 m, entrambi inclusi
Limiti	1000 m	

Impostazioni della memoria

Parametri	Valore predefinito	Intervallo configurabile
Richieste	256 Mi	Tra 256 Mi e 20000 Mi, entrambi inclusi
Limiti	1024 Mi	

Impostazioni di **`PriorityClass`**

Quando GuardDuty crea un componente aggiuntivo Amazon EKS per te, l'assegnato `PriorityClass` è`aws-guardduty-agent.priorityclass`. Ciò significa che non verrà intrapresa alcuna azione in base alla priorità del pod dell'agente. Puoi configurarlo scegliendo una delle seguenti `PriorityClass` opzioni:

Configurabile **`PriorityClass`**	**`preemptionPolicy`** value	**`preemptionPolicy`** descrizione	valore del pod
`aws-guardduty-agent.priorityclass`	`Never`	Nessuna operazione	1000000

Configurabile **PriorityClass**	**preemptionPolicy** value	**preemptionPolicy** descrizione	valore del pod
`aws-guardduty-agent.priorityclass-high`	`PreemptLowerPriority`	L'assegnazione di questo valore impedirà l'esecuzione di un pod con il valore di priorità inferiore al valore del pod dell'agente.	100000000
`system-cluster-critical` [1]	`PreemptLowerPriority`		2000000000
`system-node-critical` [1]	`PreemptLowerPriority`		2000001000

[1] Kubernetes offre queste due opzioni: e. `PriorityClass` `system-cluster-critical` `system-node-critical` Per ulteriori informazioni, consulta la documentazione di PriorityClassKubernetes.

Impostazioni di **dnsPolicy**

Scegli una delle seguenti opzioni di policy DNS supportate da Kubernetes. Quando non viene specificata alcuna configurazione, `ClusterFirst` viene utilizzato come valore predefinito.

- `ClusterFirst`
- `ClusterFirstWithHostNet`
- `Default`

Per informazioni su queste politiche, consulta la politica DNS di Pod nella documentazione di Kubernetes.

GuardDuty Implementazione di un agente di sicurezza

Questa sezione descrive come implementare il GuardDuty Security Agent per la prima volta per cluster EKS specifici. Prima di procedere con questa sezione, assicuratevi di aver già impostato i

prerequisiti e abilitato il Runtime Monitoring per i vostri account. L'agente GuardDuty di sicurezza (componente aggiuntivo EKS) non funzionerà se non abiliti il monitoraggio del runtime.

Scegliete il metodo di accesso preferito per implementare il GuardDuty security agent per la prima volta.

Console

1. Apri la console Amazon EKS all'indirizzo https://console.aws.amazon.com/eks/home#/clusters.
2. Scegli il Nome cluster.
3. Seleziona la scheda Componenti aggiuntivi.
4. Scegli Ottieni altri componenti aggiuntivi.
5. Nella pagina Seleziona componenti aggiuntivi, scegli Amazon GuardDuty Runtime Monitoring.
6. Nella pagina Configura le impostazioni dei componenti aggiuntivi selezionati, utilizza le impostazioni predefinite. Se lo stato del tuo componente aggiuntivo EKS è Richiede attivazione, scegli Attiva. GuardDuty Questa azione aprirà la GuardDuty console per configurare il monitoraggio del runtime per i tuoi account.
7. Dopo aver configurato il Runtime Monitoring per i tuoi account, torna alla console Amazon EKS. Lo Stato del componente aggiuntivo EKS dovrebbe essere stato modificato in Pronto per l'installazione.
8. (Facoltativo) Fornitura dello schema di configurazione aggiuntivo EKS

   Per la versione aggiuntiva, se si sceglie la versione 1.5.0 e successive, Runtime Monitoring supporta la configurazione di parametri specifici dell'agente. GuardDuty Per informazioni sugli intervalli di parametri, vedere. Configura i parametri aggiuntivi EKS

   a. Espandi le impostazioni di configurazione opzionali per visualizzare i parametri configurabili e il valore e il formato previsti.
   b. Imposta i parametri. I valori devono essere compresi nell'intervallo fornito inConfigura i parametri aggiuntivi EKS.
   c. Scegli Salva modifiche per creare il componente aggiuntivo in base alla configurazione avanzata.
   d. Per il metodo di risoluzione dei conflitti, l'opzione scelta verrà utilizzata per risolvere un conflitto quando si aggiorna il valore di un parametro a un valore non predefinito. Per

ulteriori informazioni sulle opzioni elencate, consulta ResolveConflicts nell'Amazon EKS API Reference.

9. Seleziona Successivo.
10. Nella pagina Rivedi e crea, verifica tutti i dettagli, quindi scegli Crea.
11. Torna ai dettagli del cluster e scegli la scheda Risorse.
12. Puoi visualizzare i nuovi pod con il prefisso. aws-guardduty-agent

API/CLI

È possibile configurare il componente aggiuntivo di Amazon EKS (`aws-guardduty-agent`) utilizzando una delle opzioni seguenti:

- Corri CreateAddonper il tuo account.
-

> **Note**
>
> Per il componente aggiuntivo`version`, se scegli la versione 1.5.0 e successive, Runtime Monitoring supporta la configurazione di parametri specifici dell'agente. GuardDuty Per ulteriori informazioni, consulta Configura i parametri aggiuntivi EKS.

Utilizza i valori seguenti per i parametri della richiesta:

- In `addonName`, immettere `aws-guardduty-agent`.

È possibile utilizzare l' AWS CLI esempio seguente quando si utilizzano valori configurabili supportati per le versioni aggiuntive v1.5.0 e successive. Assicurati di sostituire i valori segnaposto evidenziati in rosso e quelli associati ai valori configurati. `Example.json`

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

Example Esempio.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
```

```
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

- Per informazioni sulle `addonVersion` supportate, consulta Versioni di Kubernetes supportate dal security agent GuardDuty .
- In alternativa, puoi usare. AWS CLI Per ulteriori informazioni, consulta create-addon.

Aggiornamento manuale del security agent

Quando gestisci il GuardDuty security agent manualmente, hai la responsabilità di aggiornarlo per il tuo account. Per ricevere notifiche sulle nuove versioni degli agenti, puoi abbonarti a un feed RSS aGuardDuty cronologia delle versioni degli agenti.

È possibile aggiornare il Security Agent alla versione più recente per beneficiare del supporto e dei miglioramenti aggiuntivi. Se la versione corrente dell'agente sta per terminare il supporto standard, per continuare a utilizzare Runtime Monitoring (o EKS Runtime Monitoring), è necessario aggiornare la versione corrente dell'agente. Per informazioni sulle versioni di rilascio, vedereGuardDuty agente di sicurezza per cluster Amazon EKS.

Prerequisito

Prima di aggiornare la versione del Security Agent, assicurati che la versione dell'agente che intendi utilizzare ora sia compatibile con la tua versione di Kubernetes. Per ulteriori informazioni, consulta Versioni di Kubernetes supportate dal security agent GuardDuty .

Console

1. Apri la console Amazon EKS all'indirizzo https://console.aws.amazon.com/eks/home#/clusters.
2. Scegli il Nome cluster.
3. Scegli Componenti aggiuntivi.

4. In Componenti aggiuntivi, seleziona GuardDutyRuntime Monitoring.
5. Scegli Modifica per aggiornare i dettagli dell'agente.
6. Nella pagina Configura il monitoraggio del GuardDuty runtime, aggiorna i dettagli.
7. (Facoltativo) Aggiornamento dei parametri di configurazione del componente aggiuntivo

   Se la versione del componente aggiuntivo EKS è 1.5.0 o superiore, puoi anche aggiornare le impostazioni di configurazione del componente aggiuntivo.

   a. Espandi Impostazioni di configurazione opzionali per visualizzare lo schema di configurazione.
   b. Aggiorna i valori dei parametri in base all'intervallo fornito inConfigura i parametri aggiuntivi EKS.
   c. Scegli Salva modifiche per avviare l'aggiornamento.
   d. Per il metodo di risoluzione dei conflitti, l'opzione scelta verrà utilizzata per risolvere un conflitto quando si aggiorna il valore di un parametro a un valore non predefinito. Per ulteriori informazioni sulle opzioni elencate, consulta ResolveConflicts nell'Amazon EKS API Reference.

API/CLI

Per aggiornare l'agente GuardDuty di sicurezza per i tuoi cluster Amazon EKS, consulta Aggiornamento di un componente aggiuntivo.

> **Note**
>
> Per il componente aggiuntivo`version`, se scegli la versione 1.5.0 e successive, Runtime Monitoring supporta la configurazione di parametri specifici dell'agente. GuardDuty Per informazioni sugli intervalli di parametri, vedere. Configura i parametri aggiuntivi EKS

È possibile utilizzare l' AWS CLI esempio seguente quando si utilizzano valori configurabili supportati per le versioni aggiuntive v1.5.0 e successive. Assicurati di sostituire i valori segnaposto evidenziati in rosso e quelli associati ai valori configurati. `Example.json`

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

Example Esempio.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

Se la tua versione del componente aggiuntivo Amazon EKS è 1.5.0 o successiva e hai configurato lo schema del componente aggiuntivo, puoi verificare se i valori vengono visualizzati correttamente per il tuo cluster. Per ulteriori informazioni, consulta Verifica degli aggiornamenti dello schema di configurazione.

Verifica degli aggiornamenti dello schema di configurazione

Dopo aver configurato i parametri, effettuate le seguenti operazioni per verificare che lo schema di configurazione sia stato aggiornato:

1. Apri la console Amazon EKS all'indirizzo https://console.aws.amazon.com/eks/home#/clusters.
2. Nel pannello di navigazione scegliere Clusters (Cluster).
3. Nella pagina Cluster, seleziona il nome del cluster per il quale desideri verificare gli aggiornamenti.
4. Scegliere la scheda Resources (Risorse).
5. Dal riquadro Tipi di risorse, in Carichi di lavoro, scegli. DaemonSets
6. Seleziona aws-guardduty-agent.
7. Nella aws-guardduty-agentpagina, scegli Visualizzazione raw per visualizzare la risposta JSON non formattata. Verifica che i parametri configurabili visualizzino il valore che hai fornito.

Dopo la verifica, passa alla GuardDuty console. Seleziona il corrispondente Regione AWS e visualizza lo stato della copertura per i tuoi cluster Amazon EKS. Per ulteriori informazioni, consulta Copertura per i cluster Amazon EKS.

Configurazione di EKS Runtime Monitoring (solo API)

Prima di configurare il monitoraggio del runtime EKS nel tuo account, assicurati di utilizzare una delle piattaforme verificate che supporta la versione di Kubernetes attualmente in uso. Per ulteriori informazioni, consulta Convalida dei requisiti relativi all'architettura.

Configurazione del monitoraggio del runtime EKS per un account autonomo

Per gli account associati a AWS Organizations, consulta Configurazione del monitoraggio del runtime EKS per ambienti con più account.

Scegli il metodo di accesso che preferisci per abilitare il monitoraggio del runtime EKS per il tuo account.

API/CLI

In base a Approcci per gestire l'agente di sicurezza GuardDuty, puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i cluster EKS)	1. Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto `features` su `EKS_RUNTIME_MONITORING` e lo stato su `ENABLED`. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornam enti dell'agente di sicurezza per tutti i cluster Amazon EKS nel tuo account. 2. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite il tag di esclusione)	1. Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDutyManaged -false`. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con `eks:TagResource` . • Sostituisci *ec2: DeleteTags* con. `eks:UntagResource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `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. **Note** Aggiungi sempre il tag di esclusione al tuo cluster EKS prima di impostare `STATUS` of

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	`EKS_RUNTIME_MONITORING` to`ENABLED`; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account. Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto `features` su `EKS_RUNTIME_MONITORING` e lo stato su `ENABLED`. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitorare cluster EKS selettivi (utilizzando i tag di inclusione)	1. Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDutyManaged -true`. Per ulteriori informazi oni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizat ions . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con `eks:TagRe source` . • Sostituisci *ec2: DeleteTags* con. `eks:Untag Resource` • Sostituisci *access-project* con `GuardDuty Managed` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::12 3456789012:role/org-admins/iam-admin ", "arn:aws:iam::123456789012:role/org- admins/iam-admin", "arn:aws:iam::1234 56789012:role/org-admins/iam-admin"]` 3. Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto `features` su `EKS_RUNTIME_MONITORING` e lo stato su `ENABLED`.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS etichettati con la coppia `true` `GuardDutyManaged` -. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestire l'agente di sicurezza manualmente	1. Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto `features` su `EKS_RUNTIME_MONITORING` e lo stato su `ENABLED`. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. In alternativa, è possibile utilizzare il AWS CLI comando utilizzando il proprio ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `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. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Configurazione del monitoraggio del runtime EKS per ambienti con più account

In ambienti con più account, solo l'account GuardDuty amministratore delegato può abilitare o disabilitare EKS Runtime Monitoring per gli account membro e gestire la gestione degli GuardDuty agenti per i cluster EKS appartenenti agli account membro della rispettiva organizzazione. GuardDuty

Gli account membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce gli account dei membri utilizzando AWS Organizations. Per ulteriori informazioni sugli ambienti multi-account, consulta Gestione di più account.

Configurazione di EKS Runtime Monitoring per l'account amministratore delegato GuardDuty

Scegliete il metodo di accesso preferito per abilitare EKS Runtime Monitoring e gestire il GuardDuty security agent per i cluster EKS che appartengono all'account amministratore delegato GuardDuty .

API/CLI

In base a Approcci per gestire l'agente di sicurezza GuardDuty, puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i cluster EKS)	Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto `features` su `EKS_RUNTIME_MONITORING` e lo stato su `ENABLED`. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS nel tuo account. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING",`

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	`"Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'`

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite il tag di esclusione)	1. Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDutyManaged -false`. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con `eks:TagResource` . • Sostituisci *ec2: DeleteTags* con. `eks:UntagResource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `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. **Note** Aggiungi sempre il tag di esclusione al tuo cluster EKS prima di impostare `STATUS` of

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	`EKS_RUNTIME_MONITORING` to`ENABLED`; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account. Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto `features` su `EKS_RUNTIME_MONITORING` e lo stato su `ENABLED`. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitorare cluster EKS selettivi (utilizzando i tag di inclusione)	1. Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDutyManaged -true`. Per ulteriori informazi oni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizat ions . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con `eks:TagRe source` . • Sostituisci *ec2: DeleteTags* con. `eks:Untag Resource` • Sostituisci *access-project* con `GuardDuty Managed` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::12 3456789012:role/org-admins/iam-admin ", "arn:aws:iam::123456789012:role/org- admins/iam-admin", "arn:aws:iam::1234 56789012:role/org-admins/iam-admin"]` 3. Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto `features` su `EKS_RUNTIME_MONITORING` e lo stato su `ENABLED`.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS etichettati con la coppia `true` `GuardDutyManaged` -. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Gestire l'agente di sicurezza manualmente	1. Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto `features` su `EKS_RUNTIME_MONITORING` e lo stato su `ENABLED`. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. In alternativa, è possibile utilizzare il AWS CLI comando utilizzando il proprio ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'` 2. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Abilitare automaticamente il monitoraggio del runtime EKS per tutti gli account membri

Scegli il metodo di accesso che preferisci per abilitare il monitoraggio del runtime EKS per tutti gli account membri, Ciò include l'account GuardDuty amministratore delegato, gli account dei membri esistenti e i nuovi account che entrano a far parte dell'organizzazione. Scegliete il vostro approccio

preferito per gestire gli agenti di GuardDuty sicurezza per i cluster EKS che appartengono a questi account membri.

API/CLI

In base a Approcci per gestire l'agente di sicurezza GuardDuty, puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per gestire gli agenti GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i cluster EKS)	Per abilitare in modo selettivo il monitoraggio del runtime EKS per i tuoi account membri, esegui l'operazione API updateMemberDetectors utilizzando il tuo *ID rilevatore* . Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS nel tuo account. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `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"}] ]'`

Approccio preferito per gestire gli agenti GuardDuty di sicurezza	Fasi
	Note Puoi anche trasmettere un elenco di ID account separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire gli agenti GuardDuty di sicurezza	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite il tag di esclusione)	1. Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDuty Managed -false`. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con `eks:TagResource` . • Sostituisci *ec2: DeleteTags* con. `eks:Untag Resource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `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. **Note** Aggiungi sempre il tag di esclusione al tuo cluster EKS prima di impostare `STATUS` of `EKS_RUNTIME_MONITORING` to`ENABLED`; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account.

Approccio preferito per gestire gli agenti GuardDuty di sicurezza	Fasi
	Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto `features` su `EKS_RUNTIME_MONITORING` e lo stato su `ENABLED`. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `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** Puoi anche trasmettere un elenco di ID account separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica

Approccio preferito per gestire gli agenti GuardDuty di sicurezza	Fasi
	qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire gli agenti GuardDuty di sicurezza	Fasi
Monitorare cluster EKS selettivi (utilizzando i tag di inclusione)	1. Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDuty Managed -true`. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con `eks:TagResource` . • Sostituisci *ec2: DeleteTags* con. `eks:Untag Resource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `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. Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto `features` su `EKS_RUNTIME_MONITORING` e lo stato su `ENABLED`. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`.

Approccio preferito per gestire gli agenti GuardDuty di sicurezza	Fasi
	GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS etichettati con la `true` coppia `GuardDutyManaged` -. In alternativa, puoi utilizzare il AWS CLI comando utilizzan do il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `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" : " DISABLED"}] ]'` **Note** Puoi anche trasmettere un elenco di ID account separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire gli agenti GuardDuty di sicurezza	Fasi
Gestire l'agente di sicurezza manualmente	1. Esegui l'API updateDetector utilizzando il tuo ID rilevatore regionale e impostando il nome dell'oggetto `features` su `EKS_RUNTIME_MONITORING` e lo stato su `ENABLED`. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. In alternativa, è possibile utilizzare il AWS CLI comando utilizzando il proprio ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `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" : " ENABLED"}] } ]'` 2. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Configurazione del monitoraggio del runtime EKS per tutti gli account membri attivi esistenti

Scegliete il metodo di accesso preferito per abilitare EKS Runtime Monitoring e gestire l'agente di GuardDuty sicurezza per gli account dei membri attivi esistenti nella vostra organizzazione.

API/CLI

In base a Approcci per gestire l'agente di sicurezza GuardDuty, puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i cluster EKS)	Per abilitare in modo selettivo il monitoraggio del runtime EKS per i tuoi account membri, esegui l'operazione API updateMemberDetectors utilizzando il tuo *ID rilevatore* . Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS nel tuo account. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `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** Puoi anche trasmettere un elenco di ID account separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite il tag di esclusione)	1. Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDuty Managed -false`. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con `eks:TagResource` . • Sostituisci *ec2: DeleteTags* con. `eks:Untag Resource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `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. **Note** Aggiungi sempre il tag di esclusione al tuo cluster EKS prima di impostare `STATUS` of `EKS_RUNTIME_MONITORING` to`ENABLED`; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Per abilitare in modo selettivo il monitoraggio del runtime EKS per i tuoi account membri, esegui l'operazione API updateMemberDetectors utilizzando il tuo *ID rilevatore* . Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `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** Puoi anche trasmettere un elenco di ID account separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitorare cluster EKS selettivi (utilizzando i tag di inclusione)	1. Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDuty Managed -true`. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con `eks:TagResource` . • Sostituisci *ec2: DeleteTags* con. `eks:Untag Resource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `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. Per abilitare in modo selettivo il monitoraggio del runtime EKS per i tuoi account membri, esegui l'operazione API updateMemberDetectors utilizzando il tuo *ID rilevatore* . Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS etichettati con la `true` coppia `GuardDutyManaged` -. In alternativa, puoi utilizzare il AWS CLI comando utilizzan do il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `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" : " DISABLED"}] ]'` **Note** Puoi anche trasmettere un elenco di ID account separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestire l'agente di sicurezza manualmente	1. Per abilitare in modo selettivo il monitoraggio del runtime EKS per i tuoi account membri, esegui l'operazione API updateMemberDetectors utilizzando il tuo *ID rilevatore* . Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. In alternativa, è possibile utilizzare il AWS CLI comando utilizzando il proprio ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `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" : " ENABLED"}] } ]'` 2. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Abilitare automaticamente il monitoraggio del runtime EKS per i nuovi membri

L'account GuardDuty amministratore delegato può abilitare automaticamente EKS Runtime Monitoring e scegliere un approccio per la gestione del GuardDuty security agent per i nuovi account che entrano a far parte dell'organizzazione.

API/CLI

In base a Approcci per gestire l'agente di sicurezza GuardDuty, puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i cluster EKS)	Per abilitare in modo selettivo il monitoraggio del runtime EKS per i tuoi nuovi account, richiama l'operazione API UpdateOrganizationConfiguration utilizzando il tuo *ID rilevatore* . Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS nel tuo account. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `EKS_ADDON_MANAGEMENT` per un singolo account. Puoi anche trasmettere un elenco di ID account separati da uno spazio. Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --feature`

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	s '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfigu ration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}]]' Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite il tag di esclusione)	1. Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDutyManaged -false`. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con `eks:TagResource` . • Sostituisci *ec2: DeleteTags* con. `eks:UntagResource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `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. **Note** Aggiungi sempre il tag di esclusione al tuo cluster EKS prima di impostare `STATUS` of

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	`EKS_RUNTIME_MONITORING` to`ENABLED`; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account. Per abilitare in modo selettivo il monitoraggio del runtime EKS per i tuoi nuovi account, richiama l'operazione API UpdateOrganizationConfiguration utilizzando il tuo *`ID rilevatore`* . Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `EKS_ADDON_MANAGEMENT` per un singolo account. Puoi anche trasmettere un elenco di ID account separati da uno spazio. Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	`` aws guardduty update-organization-configu ration --detector-id 12abc34d567e8fa901 bc2d34e56789f0 --autoEnable --feature s '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfigu ration" : [{"Name" : "EKS_ADDON_MANAGEM ENT", "AutoEnable": "NEW"}]]' ``` Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitorare cluster EKS selettivi (utilizzando i tag di inclusione)	1. Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDutyManaged -true`. Per ulteriori informazi oni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizat ions . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con `eks:TagRe source` . • Sostituisci *ec2: DeleteTags* con. `eks:Untag Resource` • Sostituisci *access-project* con `GuardDuty Managed` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::12 3456789012:role/org-admins/iam-admin ", "arn:aws:iam::123456789012:role/org- admins/iam-admin", "arn:aws:iam::1234 56789012:role/org-admins/iam-admin"]` 3. Per abilitare in modo selettivo il monitoraggio del runtime EKS per i tuoi nuovi account, richiama l'operazione API UpdateOrganizationConfiguration utilizzando il tuo *ID rilevatore* .

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS etichettati con la coppia `GuardDutyManaged = true`. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. Nell'esempio seguente viene abilitato `EKS_RUNTIME_MONITORING` e disabilitato `EKS_ADDON_MANAGEMENT` per un singolo account. Puoi anche trasmettere un elenco di ID account separati da uno spazio. Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'`

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Gestire l'agente di sicurezza manualmente	1. Per abilitare in modo selettivo il monitoraggio del runtime EKS per i tuoi nuovi account, richiama l'operazione API UpdateOrganizationConfiguration utilizzando il tuo *ID rilevatore* . Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. In alternativa, è possibile utilizzare il AWS CLI comando utilizzando il proprio ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. Nell'esempio seguente viene abilitato `EKS_RUNTIME_MONITORING` e disabilitato `EKS_ADDON_MANAGEMENT` per un singolo account. Puoi anche trasmettere un elenco di ID account separati da uno spazio. Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` .

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema. 2. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Abilitare il monitoraggio del runtime EKS per singoli account membri attivi

API/CLI

In base a Approcci per gestire l'agente di sicurezza GuardDuty, puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i cluster EKS)	Per abilitare in modo selettivo il monitoraggio del runtime EKS per i tuoi account membri, esegui l'operazione API updateMemberDetectors utilizzando il tuo *ID rilevatore* . Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS nel tuo account. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `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** Puoi anche trasmettere un elenco di ID account separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitorare tutti i cluster EKS escludendone alcuni (tramite il tag di esclusione)	1. Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDutyManaged -false`. Per ulteriori informazioni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con `eks:TagResource` . • Sostituisci *ec2: DeleteTags* con. `eks:UntagResource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `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. **Note** Aggiungi sempre il tag di esclusione al tuo cluster EKS prima di impostare `STATUS` of

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	`EKS_RUNTIME_MONITORING` to`ENABLED`; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i cluster EKS del tuo account. Per abilitare in modo selettivo il monitoraggio del runtime EKS per i tuoi account membri, esegui l'operazione API updateMemberDetectors utilizzando il tuo *ID rilevatore* . Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `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"}] ]'`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	> **Note** > Puoi anche trasmettere un elenco di ID account separati da uno spazio. Se il codice viene eseguito correttamente, restituis ce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitorare cluster EKS selettivi (utilizzando i tag di inclusione)	1. Aggiungi un tag al cluster EKS che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDutyManaged -true`. Per ulteriori informazi oni sull'aggiunta del tag, consulta Utilizzo di tag tramite la CLI, l'API o eksctl nella Guida per l'utente di Amazon EKS. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizat ions . Sostituisci i seguenti dettagli nella policy: • Sostituisci *ec2: CreateTags* con `eks:TagResource` . • Sostituisci *ec2: DeleteTags* con. `eks:UntagResource` • Sostituisci *access-project* con `GuardDutyManaged` • Sostituisci *123456789012* con l' Account AWS ID dell'entità affidabile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `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. Per abilitare in modo selettivo il monitoraggio del runtime EKS per i tuoi account membri, esegui l'operazione API updateMemberDetectors utilizzando il tuo *ID rilevatore* .

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti dell'agente di sicurezza per tutti i cluster Amazon EKS etichettati con la coppia `GuardDutyManaged = true`. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `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" : " DISABLED"}] ]'` **Note** Puoi anche trasmettere un elenco di ID account separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.
Gestire l'agente di sicurezza manualmente	1. Per abilitare in modo selettivo il monitoraggio del runtime EKS per i tuoi account membri, esegui l'operazione API updateMemberDetectors utilizzando il tuo *ID rilevatore* . Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. In alternativa, è possibile utilizzare il AWS CLI comando utilizzando il proprio ID regionale del rilevatore. Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `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" : " ENABLED"}] } ]'` 2. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il cluster Amazon EKS.

Migrazione da EKS Runtime Monitoring a Runtime Monitoring

Con il lancio di GuardDuty Runtime Monitoring, la copertura per il rilevamento delle minacce è stata estesa ai contenitori Amazon ECS e alle istanze Amazon EC2. EKS Runtime Monitoring è stato ora consolidato in Runtime Monitoring. Puoi abilitare il monitoraggio del runtime e gestire singoli agenti di GuardDuty sicurezza per ogni tipo di risorsa (istanza Amazon EC2, cluster Amazon ECS e cluster Amazon EKS) per cui desideri monitorare il comportamento di runtime.

Non esiste un'esperienza di GuardDuty console separata per EKS Runtime Monitoring. Per continuare a utilizzare EKS Runtime Monitoring, è necessario configurarlo utilizzando le API o il AWS Command Line Interface.

Per migrare da EKS Runtime Monitoring a Runtime Monitoring

1. La GuardDuty console supporta EKS Runtime Monitoring come parte del Runtime Monitoring.

   Puoi iniziare a utilizzare Runtime Monitoring in base Verifica dello stato della configurazione del monitoraggio di EKS Runtime alla tua organizzazione e ai tuoi account.

   Assicuratevi di non disabilitare EKS Runtime Monitoring prima di abilitare Runtime Monitoring. Se disabiliti EKS Runtime Monitoring, verrà disabilitata anche la gestione dei componenti aggiuntivi di Amazon EKS. Continua con i seguenti passaggi nell'ordine indicato.
2. Assicurati di soddisfare tutti iPrerequisiti per abilitare il monitoraggio del runtime.
3. Abilita il monitoraggio del runtime replicando le stesse impostazioni di configurazione dell'organizzazione per il monitoraggio del runtime utilizzate per EKS Runtime Monitoring. Per ulteriori informazioni, consulta Abilitazione del monitoraggio del runtime.
   - Se disponi di un account autonomo, devi abilitare il Runtime Monitoring.

     Se il GuardDuty security agent è già distribuito, le impostazioni corrispondenti vengono replicate automaticamente e non è necessario configurarle nuovamente.
   - Se hai un'organizzazione con impostazioni di attivazione automatica, assicurati di replicare le stesse impostazioni di attivazione automatica per Runtime Monitoring.
   - Se hai un'organizzazione con impostazioni configurate singolarmente per gli account dei membri attivi esistenti, assicurati di abilitare il Runtime Monitoring e di configurare il GuardDuty security agent per questi membri singolarmente.
4. Dopo esserti assicurato che le impostazioni del Runtime Monitoring e del GuardDuty security agent siano corrette, disabilita EKS Runtime Monitoring utilizzando l'API o il AWS CLI comando.

5. (Facoltativo) se desideri pulire qualsiasi risorsa associata al GuardDuty security agent, consultaPulizia delle risorse del Security Agent GuardDuty .

Se desideri continuare a utilizzare EKS Runtime Monitoring senza abilitare il Runtime Monitoring, consultaConfigurazione di EKS Runtime Monitoring (solo API).

Verifica dello stato della configurazione del monitoraggio di EKS Runtime

Utilizza le seguenti API o AWS CLI comandi per verificare lo stato di configurazione esistente di EKS Runtime Monitoring.

Per verificare lo stato di configurazione di EKS Runtime Monitoring esistente nel tuo account

- Esegui GetDetectorper controllare lo stato di configurazione del tuo account.
- In alternativa, puoi eseguire il seguente comando utilizzando AWS CLI:

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1
```

Assicurati di sostituire l'ID del rilevatore della tua regione Account AWS e di quella attuale. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

Per verificare lo stato di configurazione di EKS Runtime Monitoring esistente per la vostra organizzazione (solo come account GuardDuty amministratore delegato)

- Esegui DescribeOrganizationConfigurationper verificare lo stato di configurazione della tua organizzazione.

  In alternativa, puoi eseguire il seguente comando usando AWS CLI:

```
aws guardduty describe-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
```

  Assicurati di sostituire l'ID del rilevatore con l'ID del tuo account GuardDuty amministratore delegato e la regione con la regione corrente. Per trovare i dati relativi `detectorId` al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

Disattivazione di EKS Runtime Monitoring dopo la migrazione a Runtime Monitoring

Dopo esserti assicurato che le impostazioni esistenti per il tuo account o la tua organizzazione siano state replicate su Runtime Monitoring, puoi disabilitare EKS Runtime Monitoring.

Per disabilitare EKS Runtime Monitoring

- Per disabilitare EKS Runtime Monitoring nel proprio account

  Esegui l'UpdateDetectorAPI con il tuo *detector-id* regionale.

  In alternativa, puoi usare il seguente comando. AWS CLI *Sostituisci 12abc34d567e8fa901bc2d34e56789f0 con il tuo ID rilevatore regionale.*

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

- Per disabilitare EKS Runtime Monitoring per gli account dei membri dell'organizzazione

  Esegui l'UpdateMemberDetectorsAPI con l'*ID rilevatore* regionale dell'account GuardDuty amministratore delegato dell'organizzazione.

  In alternativa, puoi usare il seguente comando. AWS CLI *Sostituisci 12abc34d567e8fa901bc2d34e56789f0 con l'ID rilevatore regionale dell'account amministratore delegato GuardDuty dell'organizzazione e 111122223333 con l'ID dell'account membro per il quale desideri disabilitare questa funzione.* Account AWS

  ```
  aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
   --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",
   "Status" : "DISABLED"}]'
  ```

- Per aggiornare EKS Runtime Monitoring, abilita automaticamente le impostazioni per la tua organizzazione

  Eseguite il passaggio seguente solo se avete configurato le impostazioni di attivazione automatica di EKS Runtime Monitoring per gli account nuovi (`NEW`) o per tutti (`ALL`) i membri dell'organizzazione. Se l'hai già configurato come`NONE`, puoi saltare questo passaggio.

> **Note**
>
> L'impostazione della configurazione di attivazione automatica di EKS Runtime Monitoring `NONE` significa che EKS Runtime Monitoring non verrà abilitato automaticamente per nessun account membro esistente o quando un nuovo account membro si unisce all'organizzazione.

Eseguite l'UpdateOrganizationConfigurationAPI con il *detector-id regionale dell'account* amministratore delegato dell'organizzazione. GuardDuty

In alternativa, puoi usare il seguente comando. AWS CLI *Sostituisci 12abc34d567e8fa901bc2d34e56789f0 con il detector-id regionale dell'account amministratore delegato dell'organizzazione.* GuardDuty Sostituisci *EXISTING_VALUE* con la configurazione corrente per l'attivazione automatica. GuardDuty

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
```

Pulizia delle risorse del Security Agent GuardDuty

È necessario eliminare le risorse negli scenari seguenti:

Quando si disabilita la configurazione automatizzata dell'agente

GuardDuty non rimuove il security agent distribuito sulla tua risorsa. Tuttavia, GuardDuty smetterà di gestire gli aggiornamenti del security agent.

GuardDuty continua a ricevere gli eventi di runtime dal tipo di risorsa in uso. Per evitare un impatto sulle statistiche di utilizzo, assicurati di rimuovere il GuardDuty security agent dalla tua risorsa.

Indipendentemente dal fatto che un Account AWS utente utilizzi o meno un endpoint VPC condiviso, GuardDuty non elimina l'endpoint VPC. Se necessario, dovrai eliminare l'endpoint VPC manualmente.

Quando disabiliti Runtime Monitoring o EKS Runtime Monitoring

In generale, GuardDuty elimina l'endpoint VPC che aveva creato. GuardDuty li contrassegna come:. `GuardDutyManaged` `true` Tuttavia, quando si disabilita il Runtime Monitoring o EKS Runtime Monitoring per un account partecipante VPC condiviso, se l'endpoint VPC condiviso è stato utilizzato da almeno un account partecipante, non GuardDuty elimina né l'endpoint VPC né il gruppo di sicurezza associato alla risorsa VPC condivisa.

Quando smetti di gestire manualmente il security agent

Indipendentemente dall'approccio utilizzato per distribuire e gestire il GuardDuty security agent, per interrompere il monitoraggio degli eventi di runtime nella risorsa, è necessario rimuovere il GuardDuty security agent. Se desideri interrompere il monitoraggio degli eventi di runtime da un tipo di risorsa in un account, puoi anche eliminare l'endpoint Amazon VPC.

Processo di pulizia delle risorse degli agenti di sicurezza

Per eliminare l'endpoint Amazon VPC

- Senza un VPC condiviso: quando non desideri più monitorare una risorsa in un account, prendi in considerazione l'eliminazione dell'endpoint Amazon VPC.
- Con un VPC condiviso: quando l'account proprietario del VPC condiviso elimina la risorsa VPC condivisa, qualsiasi account partecipante che attualmente utilizza l'endpoint VPC condiviso, lo stato di copertura del Runtime Monitoring per le risorse nell'account proprietario del VPC condiviso e nell'account partecipante potrebbe non essere integro. Per ulteriori informazioni, consulta Valutazione della copertura in fase di esecuzione delle risorse.

Per ulteriori informazioni, consulta Eliminazione di un endpoint dell'interfaccia.

Per eliminare il gruppo di sicurezza

- Senza un VPC condiviso: quando non desideri più monitorare un tipo di risorsa in un account, prendi in considerazione l'eliminazione del gruppo di sicurezza associato ad Amazon VPC.
- Con un VPC condiviso: quando l'account proprietario del VPC condiviso elimina il gruppo di sicurezza, qualsiasi account partecipante che attualmente utilizza il gruppo di sicurezza associato al VPC condiviso, lo stato di copertura del Runtime Monitoring per le risorse nell'account proprietario del VPC condiviso e nell'account partecipante potrebbe non essere integro. Per ulteriori informazioni, consulta Valutazione della copertura in fase di esecuzione delle risorse.

Per ulteriori informazioni, consulta Eliminare un gruppo di sicurezza.

Per rimuovere un agente GuardDuty di sicurezza da un cluster EKS

Per rimuovere l'agente di sicurezza dal cluster EKS che non desideri più monitorare, consulta Eliminazione di un componente aggiuntivo.

La rimozione dell'agente (componente aggiuntivo EKS) non rimuove lo spazio dei nomi di `amazon-guardduty` dal cluster EKS. Per eliminare lo spazio dei nomi `amazon-guardduty`, consulta Eliminazione di uno spazio dei nomi.

Per eliminare lo spazio dei **`amazon-guardduty`** nomi (cluster EKS)

La disabilitazione della configurazione automatizzata dell'agente non rimuove automaticamente lo spazio dei `amazon-guardduty` nomi dal cluster EKS. Per eliminare lo spazio dei nomi `amazon-guardduty`, consulta Eliminazione di uno spazio dei nomi.

Valutazione della copertura in fase di esecuzione delle risorse

Dopo aver abilitato il Runtime Monitoring e aver installato il GuardDuty security agent sulla risorsa, GuardDuty fornisce le statistiche di copertura per il tipo di risorsa corrispondente e lo stato di copertura individuale per le risorse che appartengono al tuo account. Lo stato della copertura viene determinato assicurandoti di aver abilitato il Runtime Monitoring, che l'endpoint Amazon VPC sia stato creato e che sia stato GuardDuty distribuito il security agent per la risorsa corrispondente. Uno stato di copertura integro indica che, quando si verifica un evento di runtime relativo alla risorsa, GuardDuty è in grado di ricevere tale evento di runtime tramite l'endpoint Amazon VPC e monitorarne il comportamento. Se si è verificato un problema al momento della configurazione del Runtime Monitoring, della creazione di un endpoint Amazon VPC o GuardDuty della distribuzione del security agent, lo stato di copertura appare come Non integro. Quando lo stato di copertura non è integro, non GuardDuty sarà in grado di ricevere o monitorare il comportamento di runtime della risorsa corrispondente o generare alcun risultato di Runtime Monitoring.

I seguenti argomenti ti aiuteranno a rivedere le statistiche sulla copertura, configurare EventBridge le notifiche e risolvere i problemi di copertura per un tipo di risorsa specifico.

Indice

- Copertura per l'istanza Amazon EC2
- Copertura per la risorsa Fargate (solo Amazon ECS)
- Copertura per i cluster Amazon EKS
- Domande frequenti (FAQ)

Copertura per l'istanza Amazon EC2

Per una risorsa Amazon EC2, la copertura del runtime viene valutata a livello di istanza. Le tue istanze Amazon EC2 possono eseguire diversi tipi di applicazioni e carichi di lavoro, tra gli altri, nel tuo ambiente. AWS Questa funzionalità supporta anche le istanze Amazon EC2 gestite da Amazon ECS e se hai cluster Amazon ECS in esecuzione su un'istanza Amazon EC2, i problemi di copertura a livello di istanza verranno visualizzati nella copertura del runtime di Amazon EC2.

Argomenti

- Revisione delle statistiche di copertura
- Configurazione delle notifiche delle modifiche dello stato di copertura
- Risoluzione dei problemi di copertura

Revisione delle statistiche di copertura

Le statistiche di copertura per le istanze Amazon EC2 associate ai tuoi account o ai tuoi account membro sono la percentuale delle istanze EC2 integre rispetto a tutte le istanze EC2 selezionate. Regione AWS L'equazione seguente rappresenta questa percentuale come:

(Istanze integre/Tutte le istanze) *100

Se hai anche distribuito l'agente di GuardDuty sicurezza per i tuoi cluster Amazon ECS, qualsiasi problema di copertura a livello di istanza associato ai cluster Amazon ECS in esecuzione su un'istanza Amazon EC2 verrà visualizzato come un problema di copertura del runtime dell'istanza Amazon EC2.

Scegli uno dei metodi di accesso per esaminare le statistiche di copertura dei tuoi account.

Console

- Accedi e apri la console all'indirizzo https://console.aws.amazon.com/guardduty/. AWS Management Console GuardDuty
- Nel pannello di navigazione, scegli Runtime Monitoring.
- Scegli la scheda Runtime coverage.
- Nella scheda Copertura del runtime dell'istanza EC2, puoi visualizzare le statistiche di copertura aggregate in base allo stato di copertura di ogni istanza Amazon EC2 disponibile nella tabella Elenco istanze.
  - Puoi filtrare la tabella dell'elenco delle istanze in base alle seguenti colonne:

    - ID account
    - Tipo di gestione dell'agente
    - Versione dell'agente
    - Stato copertura
    - ID dell'istanza
    - ARN del cluster
- Se una delle tue istanze EC2 ha lo stato di copertura come Non integro, la colonna Problema include informazioni aggiuntive sul motivo dello stato Non integro.

API/CLI

- Esegui l'ListCoverageAPI con il tuo ID rilevatore, la tua regione corrente e l'endpoint di servizio validi. Puoi filtrare e ordinare l'elenco delle istanze utilizzando questa API.
    - Puoi modificare il `filter-criteria` di esempio con una delle opzioni seguenti per `CriterionKey`:
        - `ACCOUNT_ID`
        - `RESOURCE_TYPE`
        - `COVERAGE_STATUS`
        - `AGENT_VERSION`
        - `MANAGEMENT_TYPE`
        - `INSTANCE_ID`
        - `CLUSTER_ARN`
    - Quando `filter-criteria` include `RESOURCE_TYPE` EC2, Runtime Monitoring non supporta l'uso di ISSUE come. `AttributeName` Se lo usi, la risposta dell'API risulterà. `InvalidInputException`

      Puoi modificare il `AttributeName` di esempio in `sort-criteria` con una delle opzioni seguenti:

        - `ACCOUNT_ID`
        - `COVERAGE_STATUS`
        - `INSTANCE_ID`
        - `UPDATED_AT`

- Puoi modificare il numero di *max-results* (fino a 50).
- Per trovare le detectorId informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
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
```

- Esegui l'GetCoverageStatisticsAPI per recuperare le statistiche aggregate sulla copertura basate su. statisticsType
  - Puoi modificare il statisticsType di esempio con una delle opzioni seguenti:
    - COUNT_BY_COVERAGE_STATUS: rappresenta le statistiche di copertura per i cluster EKS aggregate per stato di copertura.
    - COUNT_BY_RESOURCE_TYPE— Statistiche di copertura aggregate in base al tipo di AWS risorsa nell'elenco.
    - È possibile modificare il filter-criteria di esempio nel comando. Puoi utilizzare le seguenti opzioni per CriterionKey:
      - ACCOUNT_ID
      - RESOURCE_TYPE
      - COVERAGE_STATUS
      - AGENT_VERSION
      - MANAGEMENT_TYPE
      - INSTANCE_ID
      - CLUSTER_ARN
  - Per trovare le detectorId informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
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"}}] }'
```

Se lo stato di copertura della tua istanza EC2 è Inadeguato, consulta. Risoluzione dei problemi di copertura

Configurazione delle notifiche delle modifiche dello stato di copertura

Lo stato di copertura dell'istanza Amazon EC2 potrebbe apparire come Non integro. Per sapere quando lo stato della copertura cambia, ti consigliamo di monitorare periodicamente lo stato della copertura e di risolvere i problemi se lo stato diventa Non integro. In alternativa, puoi creare una EventBridge regola Amazon per ricevere una notifica quando lo stato della copertura cambia da Insalutare a Healthy o altro. Per impostazione predefinita, GuardDuty lo pubblica nel EventBridge bus relativo al tuo account.

Schema di esempio delle notifiche

EventBridge Di norma, è possibile utilizzare gli eventi e i modelli di eventi di esempio predefiniti per ricevere notifiche sullo stato della copertura. Per ulteriori informazioni sulla creazione di una EventBridge regola, consulta Create rule nella Amazon EventBridge User Guide.

Inoltre, puoi creare un pattern di eventi personalizzato utilizzando lo schema di esempio delle notifiche seguente. Assicurati di sostituire i valori per il tuo account. Per ricevere una notifica quando lo stato di copertura della tua istanza Amazon EC2 cambia da `Healthy` a`Unhealthy`, `detail-type` deve essere *`GuardDuty Runtime Protection`* Unhealthy. Per ricevere una notifica quando lo stato di copertura cambia da `Unhealthy` a`Healthy`, sostituisci il valore di `detail-type` con *`GuardDuty Runtime Protection`* Healthy.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Account AWS ID",
  "time": "event timestamp (string)",
  "region": "Regione 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"
  }
}
```

Risoluzione dei problemi di copertura

Se lo stato di copertura della tua istanza Amazon EC2 non è integro, puoi visualizzare il motivo nella colonna Problema.

La tabella seguente elenca i tipi di problemi e i passaggi di risoluzione corrispondenti.

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
Nessuna segnalazione da parte dell'agente	In attesa di una notifica via SMS	Assicurati che l'istanza Amazon EC2 sia già gestita tramite SSM. La ricezione della notifica SSM potrebbe richiedere alcuni minuti.
	(Vuoto apposta)	Se si gestisce il GuardDuty Security Agent manualmente, questa operazione non è utilizzabile.
		Se hai abilitato la configurazione automatica dell'agente: • La tua istanza EC2 è gestita tramite SSM. • Visualizza periodicamente lo stato del tuo agente di sicurezza. Per ulteriori informazioni, consulta Convalida dello stato di installazione del GuardDuty Security Agent.

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
	Agente disconnesso	• Visualizza lo stato del tuo agente di sicurezza. Per ulteriori informazioni, consulta Convalida dello stato di installazione del GuardDuty Security Agent. • Visualizza i log del Security Agent per identificare la potenziale causa principale. I log forniscono errori dettagliati che è possibile utilizzare per risolvere autonomamente il problema. I file di registro sono disponibili in. `/var/log/amzn-guardduty-agent/` Fare `sudo journalctl -u amazon-guardduty-agent` .
Creazione dell'associazione SSM non riuscita	GuardDuty L'associazione SSM esiste già nel tuo account	1. Elimina manualmente l'associazione esistente. Per ulteriori informazioni, vedere Eliminazione delle associazioni nella Guida per l'AWS Systems Manager utente. 2. Dopo aver eliminato l'associazione, disabilita e riattiva la configurazione GuardDuty automatica dell'agente per Amazon EC2.
	Il tuo account ha troppe associazioni SSM	Scegli una delle due opzioni seguenti: • Eliminare tutte le associazioni SSM non utilizzate. Per ulteriori informazioni, consulta Eliminazione delle associazioni nella Guida per l'AWS Systems Manager utente. • Verifica se il tuo account è idoneo per un aumento della quota. Per ulteriori informazioni, vedere le quote del servizio Systems Manager nel Riferimenti generali di AWS.

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
Aggiornamento dell'associazione SSM non riuscito	GuardDuty L'associazione SSM non esiste nel tuo account	L'associazione SSM è mancante. Disabilita e riattiva il monitoraggio del runtime.
Eliminazione dell'associazione SSM non riuscita	GuardDuty L'associazione SSM non esiste nel tuo account	L'associazione SSM è mancante. Questo non è utilizzabile.
Esecuzione dell'associazione di istanze SSM non riuscita	I requisiti architettonici o altri prerequisiti non sono soddisfatti.	Per informazioni sulle distribuzioni verificate del sistema operativo, vedere. Prerequisiti per il supporto delle istanze Amazon EC2 Se il problema persiste, i seguenti passaggi ti aiuteranno a identificare e potenzialmente risolvere il problema: 1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/. 2. Nel riquadro di navigazione, in Gestione dei nodi, seleziona State Manager. 3. Filtra per proprietà Document Name e inserisci AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin. 4. Seleziona l'ID dell'associazione corrispondente e visualizzane la cronologia di esecuzione. 5. Utilizzando la cronologia di esecuzione, visualizza gli errori, identifica la potenziale causa principale e prova a risolverla.

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
Creazione degli endpoint VPC non riuscita	La creazione dell'endpoint VPC non è supportata per il VPC condiviso *vpcId*	Il Runtime Monitoring supporta l'uso di un VPC condiviso all'interno di un'organizzazione. Per ulteriori informazioni, consulta Utilizzo di VPC condiviso con agenti di sicurezza automatizzati.
	Solo quando si utilizza un VPC condiviso con configurazione automatizzata degli agenti L'ID dell'account proprietario *111122223333* per VPC condiviso *VPCid* non ha né il monitoraggio del runtime né la configurazione automatica dell'agente o entrambi abilitati	L'account proprietario del VPC condiviso deve abilitare il monitoraggio del runtime e la configurazione automatica degli agenti per almeno un tipo di risorsa (Amazon EKS o Amazon ECS ())AWS Fargate. Per ulteriori informazioni, consulta Prerequisiti specifici per il monitoraggio del runtime GuardDuty.

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
	Per abilitare il DNS privato è necessario che gli attributi VPC `enableDnsSupport` e `enableDnsHostnames` siano impostati su `true` per *`VPCId`* (servizio: Ec2, codice di stato: 400, ID della richiesta: *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*).	Assicurati che i seguenti attributi VPC siano impostati su `true` – `enableDnsSupport` e `enableDnsHostnames` . Per ulteriori informazioni, consulta Attributi DNS nel VPC. Se utilizzi la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/ per creare un Amazon VPC, assicurati di selezionare sia Abilita nomi host DNS che Abilita risoluzione DNS. Per ulteriori informazioni, consulta Opzioni di configurazione del VPC.

Tipo di problema	Messaggio di emissione	Fasi per la risoluzione dei problemi
Eliminazione degli endpoint VPC condivisi non riuscita	*L'eliminazione di un endpoint VPC condiviso non è consentita per l'account ID 111122223333 , il VPCid VPC condiviso , l'ID dell'account proprietario 5555.*	Potenziali passaggi: • La disabilitazione dello stato di monitoraggio del runtime dell'account partecipante VPC condiviso non influisce sulla policy degli endpoint VPC condivisi e sul gruppo di sicurezza esistente nell'account del proprietario. Per eliminare l'endpoint VPC condiviso e il gruppo di sicurezza, devi disabilitare il monitoraggio del runtime o lo stato di configurazione automatica dell'agente nell'account proprietario del VPC condiviso. • L'account partecipante VPC condiviso non può eliminare l'endpoint VPC condiviso e il gruppo di sicurezza ospitati nell'account proprietario del VPC condiviso.
L'agente non effettua la segnalazione	(Vuoto apposta)	Il tipo di problema ha raggiunto la fine del supporto. Se continui a riscontrare questo problema e non lo hai ancora fatto, abilita l'agente GuardDuty automatizzato per Amazon EC2. Se il problema persiste, prendi in considerazione la possibilità di disattivare il Runtime Monitoring per alcuni minuti, quindi riattivalo.

Copertura per la risorsa Fargate (solo Amazon ECS)

Per un cluster Amazon ECS eseguito su Fargate, la copertura del runtime viene valutata a livello di attività. La copertura del runtime dei cluster ECS include le attività Fargate che sono iniziate a essere eseguite dopo aver abilitato il monitoraggio del runtime e la configurazione automatica degli agenti.

Se l'attività Fargate era già in esecuzione quando è stato abilitato il monitoraggio del runtime, questa attività non verrà presa in considerazione per valutare la copertura del runtime dei cluster ECS. Per includere un'attività Fargate di questo tipo, è necessario interromperla ed eseguirla nuovamente.

Revisione delle statistiche di copertura

Le statistiche di copertura per le risorse AWS Fargate (solo Amazon ECS) associate ai tuoi account o ai tuoi account membro sono la percentuale di cluster Amazon ECS integri rispetto a tutti i cluster Amazon ECS selezionati. Regione AWS L'equazione seguente rappresenta questa percentuale come:

(Cluster integri/Tutti i cluster)*100

Le statistiche sulla copertura includono le attività di Fargate che sono in esecuzione o che sono state completate di recente.

Scegli uno dei metodi di accesso per esaminare le statistiche di copertura dei tuoi account.

Console

- Accedere AWS Management Console e aprire la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
- Nel pannello di navigazione, scegli Runtime Monitoring.
- Scegli la scheda Runtime coverage.
- Nella scheda Runtime Coverage dei cluster ECS, puoi visualizzare le statistiche di copertura aggregate in base allo stato di copertura di ogni cluster Amazon ECS disponibile nella tabella Elenco dei cluster.
  - Puoi filtrare la tabella dell'elenco dei cluster in base alle seguenti colonne:
    - ID account
    - Nome del cluster
    - Tipo di gestione dell'agente
    - Stato copertura
- Se uno dei tuoi cluster ECS ha lo stato di copertura impostato su Non integro, la colonna Problema include informazioni aggiuntive sul motivo dello stato Non integro.

API/CLI

- Esegui l'ListCoverageAPI con il tuo ID rilevatore, la regione corrente e l'endpoint del servizio validi. Puoi filtrare e ordinare l'elenco delle istanze utilizzando questa API.
  - Puoi modificare il `filter-criteria` di esempio con una delle opzioni seguenti per `CriterionKey`:
    - `ACCOUNT_ID`
    - `ECS_CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `MANAGEMENT_TYPE`
  - Puoi modificare il `AttributeName` di esempio in `sort-criteria` con una delle opzioni seguenti:
    - `ACCOUNT_ID`
    - `COVERAGE_STATUS`
    - `ISSUE`
    - `ECS_CLUSTER_NAME`
    - `UPDATED_AT`

      Il campo viene aggiornato solo quando viene creata una nuova attività nel cluster Amazon ECS associato o quando viene modificato lo stato di copertura corrispondente.
  - Puoi modificare il numero di *`max-results`* (fino a 50).
  - Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
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
```

- Esegui l'GetCoverageStatisticsAPI per recuperare le statistiche aggregate sulla copertura basate su. `statisticsType`
  - Puoi modificare il `statisticsType` di esempio con una delle opzioni seguenti:
    - `COUNT_BY_COVERAGE_STATUS`— Rappresenta le statistiche di copertura per i cluster ECS aggregate per stato di copertura.

    - `COUNT_BY_RESOURCE_TYPE`— Statistiche di copertura aggregate in base al tipo di AWS risorsa nell'elenco.
    - È possibile modificare il `filter-criteria` di esempio nel comando. Puoi utilizzare le seguenti opzioni per `CriterionKey`:
        - `ACCOUNT_ID`
        - `ECS_CLUSTER_NAME`
        - `COVERAGE_STATUS`
        - `MANAGEMENT_TYPE`
        - `INSTANCE_ID`
- Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
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"}}] }'
```

Per ulteriori informazioni sui problemi di copertura, consultaRisoluzione dei problemi di copertura.

Configurazione delle notifiche delle modifiche dello stato di copertura

Lo stato di copertura del tuo cluster Amazon ECS potrebbe apparire come Non integro. Per sapere quando lo stato della copertura cambia, ti consigliamo di monitorare periodicamente lo stato della copertura e di risolvere i problemi se lo stato diventa Non integro. In alternativa, puoi creare una EventBridge regola Amazon per ricevere una notifica quando lo stato della copertura cambia da Insalutare a Healthy o altro. Per impostazione predefinita, GuardDuty lo pubblica nel EventBridge bus relativo al tuo account.

Schema di esempio delle notifiche

EventBridge Di norma, è possibile utilizzare gli eventi e i modelli di eventi di esempio predefiniti per ricevere notifiche sullo stato della copertura. Per ulteriori informazioni sulla creazione di una EventBridge regola, consulta Create rule nella Amazon EventBridge User Guide.

Inoltre, puoi creare un pattern di eventi personalizzato utilizzando lo schema di esempio delle notifiche seguente. Assicurati di sostituire i valori per il tuo account. Per ricevere una notifica quando lo stato di copertura del tuo cluster Amazon ECS cambia da `Healthy` a`Unhealthy`, `detail-`

`type` dovrebbe essere *`GuardDuty Runtime Protection Unhealthy`*. Per ricevere una notifica quando lo stato della copertura cambia da `Unhealthy` a`Healthy`, sostituisci il valore di `detail-type` con *`GuardDuty Runtime Protection`* Healthy.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Account AWS ID",
  "time": "event timestamp (string)",
  "region": "Regione 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"
  }
}
```

Risoluzione dei problemi di copertura

Se lo stato di copertura del tuo cluster Amazon ECS non è integro, puoi visualizzare il motivo nella colonna Problema.

La tabella seguente fornisce i passaggi consigliati per la risoluzione dei problemi di Fargate (solo Amazon ECS).

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
L'agente non effettua la segnalazione	Agente che non effettua la segnalazione per le attività in `TaskDefinition - '` *`TASK_DEFINITION`* `'`	Verifica che la configurazione degli endpoint Amazon VPC sia corretta.
	`VPC_ISSUE` `; for task in TaskDefinition - '` *`TASK_DEFINITION`* `'`	Visualizza i dettagli del problema del VPC nelle informazioni aggiuntive.
L'agente è uscito	ExitCode: `EXIT_CODE` per le attività in `TaskDefinition - '`*`TASK_DEFINITION`*`'`	Visualizza i dettagli del problema nelle informazioni aggiuntive.
	Motivo: *`MOTIVO`* delle attività in `TaskDefinition - '` *`TASK_DEFINITION`* `'`	
	ExitCode: `EXIT_CODE` con motivo: '*`EXIT_CODE`*' per le attività in `TaskDefinition - '`*`TASK_DEFINITION`*`'`	
	Agente uscito: `MotivoCannotPullContainerError` : pull image manifest è stato riprovato...	Il ruolo di esecuzione dell'attività deve disporre delle seguenti autorizzazioni Amazon Elastic Container Registry (Amazon ECR):

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
		`` ... "ecr:GetAuthorizationToken", "ecr:BatchCheckLayerAvailability", "ecr:GetDownloadUrlForLayer", "ecr:BatchGetImage", ... ``` Per ulteriori informazioni, consulta Fornisci le autorizzazioni ECR e i dettagli della sottorete. Dopo aver aggiunto le autorizzazioni Amazon ECR, devi riavviare l'attività. Se il problema persiste, consulta. Il mio AWS Step Functions flusso di lavoro non funziona in modo imprevisto
ExitCode: `EXIT_CODE` per le attività in `TaskDefinition - '`*`TASK_DEFINITION`*` '`	Visualizza i dettagli del problema nelle informazioni aggiuntive.	
ExitCode: `EXIT_CODE` con motivo: '*`EXIT_CODE`* ' per le attività in `TaskDefinition - '`*`TASK_DEFINITION`*` '`		
Motivo: *`MOTIVO`* delle attività in `TaskDefinition - '` *`TASK_DEFINITION`*` '`		

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
L'agente non effettua la segnalazione	Agente che non effettua la segnalazione per le attività in `TaskDefinition - ' TASK_DEFINITION '`	Verifica che la configurazione degli endpoint Amazon VPC sia corretta.
	`VPC_ISSUE ; for task in TaskDefinition - ' TASK_DEFINITION '`	Visualizza i dettagli del problema del VPC nelle informazioni aggiuntive.

<table>
<tr><th>Tipo di problema</th><th>Informazioni supplementari</th><th>Fasi consigliate per la risoluzione dei problemi</th></tr>
<tr><td>Altri o agente non fornito</td><td>Problema non identificato, per le attività in <code>TaskDefinition - 'TASK_DEFINITION '</code></td><td>Utilizza le seguenti domande per identificare la causa principale del problema:<table><tr><th>Domanda</th><th>Spiegazione</th></tr><tr><td>L'attività è iniziata prima di abilitare il Runtime Monitoring?</td><td>In Amazon ECS, le attività sono immutabili. Per valutare il comportamento di runtime di un'attività Fargate in esecuzione, assicuratevi che Runtime Monitoring sia già abilitato, quindi riavviate l'attività per GuardDuty aggiungere il sidecar del contenitore.</td></tr><tr><td>L'attività è stata avviata da un servizio non supportato?</td><td>Attualmente, Runtime Monitoring non supporta le attività avviate da AWS Batch</td></tr></table></td></tr>
</table>

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi	
		Domanda	Spiegazione
			and. AWS CodePipeline
		Questa attività fa parte di una distribuzione di servizi iniziata prima dell'attivazione del Runtime Monitoring?	In caso affermativo, è possibile riavviare il servizio o aggiornarlo `forceNewDeployment` utilizzando la procedura descritta in Aggiornamento di un servizio. Puoi anche usare UpdateService o AWS CLI.
		L'attività è stata avviata dopo aver escluso il cluster ECS dal Runtime Monitoring?	Quando si modifica il GuardDuty tag predefinito da `GuardDutyManaged -true` a `GuardDutyManaged -false`, non GuardDuty riceverà gli eventi di runtime

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi	
		Domanda	Spiegazione
			per il cluster ECS.
		Nella tua attività manca un? `TaskExecutionRole`	È obbligatorio aggiungere un file `TaskExecutionRole` perché GuardDuty richiede le autorizzazioni per scaricare il GuardDuty contenitore dall'archivio ECR. Per ulteriori informazioni, consulta Fornisci le autorizzazioni ECR e i dettagli della sottorete.
		Il tuo servizio contiene un'attività che ha un vecchio formato di? `taskArn`	GuardDuty Runtime Monitoring non supporta la copertura per le attività che hanno il vecchio formato di `taskArn`.

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi	
		Domanda	Spiegazione
			Per informazioni su Amazon Resource Names (ARNs) per le risorse Amazon ECS, consulta Amazon Resource Names (ARN) e ID.

Copertura per i cluster Amazon EKS

Revisione delle statistiche di copertura

Le statistiche di copertura per i cluster EKS associati ai tuoi account o ai tuoi account membri consistono nella percentuale dei cluster EKS integri rispetto a tutti i cluster EKS nella Regione AWS selezionata. L'equazione seguente rappresenta questa percentuale come:

(Cluster integri/Tutti i cluster)*100

Scegli uno dei metodi di accesso per esaminare le statistiche di copertura dei tuoi account.

Console

- Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
- Nel pannello di navigazione, scegli Runtime Monitoring.
- Scegli la scheda Copertura runtime dei cluster EKS.
- Nella scheda Copertura runtime del cluster EKS puoi visualizzare le statistiche di copertura aggregate per stato di copertura, disponibili nella tabella Elenco cluster.
  - Puoi filtrare la tabella Elenco cluster in base alle seguenti colonne:

    - Nome cluster
    - ID account
    - Tipo di gestione dell'agente
    - Stato copertura
    - Versione del componente aggiuntivo
- Se uno dei tuoi cluster EKS ha lo Stato copertura impostato su Non integro, la colonna Problema può includere informazioni aggiuntive sul motivo dello stato Non integro.

API/CLI

- Esegui l'ListCoverageAPI con il tuo ID rilevatore, la tua regione e l'endpoint di servizio validi. Puoi filtrare e ordinare l'elenco dei cluster utilizzando l'API in questione.
    - Puoi modificare il `filter-criteria` di esempio con una delle opzioni seguenti per `CriterionKey`:
        - `ACCOUNT_ID`
        - `CLUSTER_NAME`
        - `RESOURCE_TYPE`
        - `COVERAGE_STATUS`
        - `ADDON_VERSION`
        - `MANAGEMENT_TYPE`
    - Puoi modificare il `AttributeName` di esempio in `sort-criteria` con una delle opzioni seguenti:
        - `ACCOUNT_ID`
        - `CLUSTER_NAME`
        - `COVERAGE_STATUS`
        - `ISSUE`
        - `ADDON_VERSION`
        - `UPDATED_AT`
    - Puoi modificare il numero di *`max-results`* (fino a 50).
    - Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
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
```

- Esegui l'GetCoverageStatisticsAPI per recuperare le statistiche aggregate sulla copertura basate su. `statisticsType`
  - Puoi modificare il `statisticsType` di esempio con una delle opzioni seguenti:
    - `COUNT_BY_COVERAGE_STATUS`: rappresenta le statistiche di copertura per i cluster EKS aggregate per stato di copertura.
    - `COUNT_BY_RESOURCE_TYPE`— Statistiche di copertura aggregate in base al tipo di AWS risorsa nell'elenco.
    - È possibile modificare il `filter-criteria` di esempio nel comando. Puoi utilizzare le seguenti opzioni per `CriterionKey`:
      - `ACCOUNT_ID`
      - `CLUSTER_NAME`
      - `RESOURCE_TYPE`
      - `COVERAGE_STATUS`
      - `ADDON_VERSION`
      - `MANAGEMENT_TYPE`
  - Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
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"}}] }'
```

Se lo stato di copertura del cluster EKS è Non integro, consulta Risoluzione dei problemi di copertura EKS.

Configurazione delle notifiche delle modifiche dello stato di copertura

Lo stato di copertura di un cluster EKS nel tuo account potrebbe essere visualizzato come Non integro. Per rilevare quando lo stato di copertura diventa Non integro, ti consigliamo di monitorarlo periodicamente e di risolvere i problemi se è Non integro. In alternativa, puoi creare una EventBridge regola Amazon per avvisarti quando lo stato della copertura cambia `Unhealthy` da `Healthy` o in altro modo. Per impostazione predefinita, GuardDuty lo pubblica nel EventBridgebus per il tuo account.

Schema di esempio delle notifiche

EventBridge Di norma, è possibile utilizzare gli eventi e i modelli di eventi di esempio predefiniti per ricevere notifiche sullo stato della copertura. Per ulteriori informazioni sulla creazione di una EventBridge regola, consulta Create rule nella Amazon EventBridge User Guide.

Inoltre, puoi creare un pattern di eventi personalizzato utilizzando lo schema di esempio delle notifiche seguente. Assicurati di sostituire i valori per il tuo account. Per ricevere una notifica quando lo stato di copertura del tuo cluster Amazon EKS cambia da `Healthy` a`Unhealthy`, `detail-type` dovrebbe essere *`GuardDuty Runtime Protection Unhealthy`*. Per ricevere una notifica quando lo stato della copertura cambia da `Unhealthy` a`Healthy`, sostituisci il valore di `detail-type` con *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Account AWS ID",
  "time": "event timestamp (string)",
  "region": "Regione 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"
  }
}
```

Risoluzione dei problemi di copertura EKS

Se lo stato di copertura per il tuo cluster EKS è`Unhealthy`, puoi visualizzare l'errore corrispondente nella colonna Problema della GuardDuty console o utilizzando il tipo di CoverageResourcedati.

Quando utilizzi tag di inclusione o di esclusione per monitorare in modo selettivo i cluster EKS, la sincronizzazione dei tag potrebbe richiedere del tempo. Ciò potrebbe influire sullo stato di copertura del cluster EKS associato. Puoi provare a rimuovere e aggiungere nuovamente il tag corrispondente (di inclusione o di esclusione). Per ulteriori informazioni, consulta Assegnazione di tag alle risorse Amazon EKS nella Guida per l'utente di Amazon EKS.

La struttura di un problema di copertura è `Issue type:Extra information`. In genere, in caso di problemi vengono fornite Informazioni supplementari facoltative che possono includere specifiche eccezioni o descrizioni del problema sul lato client. Sulla base di informazioni aggiuntive, le tabelle seguenti forniscono i passaggi consigliati per risolvere i problemi di copertura per i cluster EKS.

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
Creazione del componente aggiuntivo non riuscita	L'addon non `aws-guardduty-agent` è compatibile con la versione corrente del cluster in cluster. *`ClusterName`* Il componente aggiuntivo specificato non è supportato.	Assicurati di utilizzare una delle versioni di Kubernetes che supportano l'implementazione del componente aggiuntivo EKS `aws-guardduty-agent` . Per ulteriori informazioni, consulta Versioni di Kubernetes supportate dal security

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
		agent GuardDuty . Per informazioni sull'aggiornamento della versione di Kubernetes, consulta Aggiornamento di una versione Kubernetes del cluster Amazon EKS.
Creazione del componente aggiuntivo non riuscita Aggiornamento del componente aggiuntivo non riuscito Stato del componente aggiuntivo non integro	Problema relativo al componente aggiuntivo EKS - `AddonIssueCode` : `AddonIssueMessage`	Per informazioni sui passaggi consigliati per un codice di problema specifico del componente aggiuntivo, consulta. Troubleshooting steps for Addon creation/updatation error with Addon issue code Per un elenco dei codici di problema relativi ai componenti aggiuntivi che potresti riscontrare in questo problema, consulta. AddonIssue

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
Creazione dell'endpoint VPC non riuscita	*La creazione di endpoint VPC non è supportata per VPC VPCId condiviso*	Il Runtime Monitoring ora supporta l'uso di un VPC condiviso all'interno di un'organizzazione. Assicurati che i tuoi account soddisfino tutti i prerequisiti. Per ulteriori informazioni, consulta Prerequisiti per l'utilizzo di un VPC condiviso.
	Solo quando si utilizza un VPC condiviso con configurazione automatizzata degli agenti L'ID dell'account proprietario *111122223333* per VPC condiviso *VPCId* non ha né il monitoraggio del runtime né la configurazione automatica degli agenti abilitati o entrambi.	L'account proprietario del VPC condiviso deve abilitare il monitoraggio del runtime e la configurazione automatica degli agenti per almeno un tipo di risorsa (Amazon EKS o Amazon ECS ())AWS Fargate. Per ulteriori informazioni, consulta Prerequisiti specifici per il monitoraggio del runtime GuardDuty.

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
	Per abilitare il DNS privato è necessario che gli attributi VPC `enableDnsSupport` e `enableDnsHostnames` siano impostati su `true` per *`VPCId`* (servizio: Ec2, codice di stato: 400, ID della richiesta: *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*).	Assicurati che i seguenti attributi VPC siano impostati su `true` – `enableDnsSupport` e `enableDnsHostnames` . Per ulteriori informazioni, consulta Attributi DNS nel VPC. Se utilizzi la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/ per creare un Amazon VPC, assicurati di selezionare sia Abilita nomi host DNS che Abilita risoluzione DNS. Per ulteriori informazioni, consulta Opzioni di configurazione del VPC.

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
Eliminazione dell'endpoint VPC condiviso non riuscita	*L'eliminazione di un endpoint VPC condiviso non è consentita per l'account ID 111122223333 , il VPCid VPC condiviso , l'ID dell'account proprietario 5555.*	Potenziali passaggi: • La disabilitazione dello stato di monitoraggio del runtime dell'account partecipante VPC condiviso non influisce sulla policy degli endpoint VPC condivisi e sul gruppo di sicurezza esistente nell'account del proprietario. Per eliminare l'endpoint VPC condiviso e il gruppo di sicurezza , devi disabilitare il monitoraggio del runtime o lo stato di configurazione automatica dell'agente nell'account proprietario del VPC condiviso. • L'account partecipante VPC condiviso non può eliminare l'endpoint VPC condiviso e il gruppo di sicurezza ospitati nell'account proprietario del VPC condiviso.

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
Cluster EKS locali	I componenti aggiuntivi EKS non sono supportati sui cluster outpost locali.	Non utilizzabile. Per ulteriori informazioni, consulta Amazon EKS su AWS Outposts.
Autorizzazione per l'abilitazione del monitoraggio del runtime EKS non concessa	(può mostrare o meno informazioni aggiuntive)	1. Se sono disponibili informazioni supplementari per questo problema, correggine la causa principale e segui la fase successiva. 2. Disattiva il monitoraggio del runtime EKS, quindi riattivalo. Assicurati che anche l' GuardDuty agente venga distribuito, automaticamente GuardDuty o manualmente.

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
Provisioning delle risorse per l'abilitazione del monitoraggio del runtime EKS in corso	(può mostrare o meno informazioni aggiuntive)	Non utilizzabile. Dopo aver abilitato il monitoraggio del runtime EKS, lo stato di copertura potrebbe rimanere `Unhealthy` fino al completamento della fase di provisioning delle risorse. Lo stato di copertura viene monitorato e aggiornato periodicamente.
Altri (qualsiasi altro problema)	Errore dovuto a un errore di autorizzazione	Disattiva il monitoraggio del runtime EKS, quindi riattivalo. Assicurati che anche l' GuardDuty agente venga distribuito, automaticamente GuardDuty o manualmente.

Errore di creazione o aggiornamento del componente aggiuntivo	Fasi per la risoluzione dei problemi
Problema relativo all'addon EKS`InsufficientNumberOfReplicas` : il componente aggiuntivo non è integro perché non ha il numero di repliche desiderato.	Utilizzando il messaggio di problema, è possibile identificare e correggere la causa principale. Puoi iniziare descrivendo il tuo cluster. Ad esempio, `kubectl describe`

Errore di creazione o aggiornamento del componente aggiuntivo	Fasi per la risoluzione dei problemi
	pods da utilizzare per identificare la causa principale dell'errore del pod. Dopo aver corretto la causa principale, riprova il passaggio (creazione o aggiornamento del componente aggiuntivo).
EKS Addon IssueAdmissionRequestDenied : il webhook di ammissione "validate.kyverno.svc-fail" ha respinto la richiesta: politica DaemonSet/amazon-guardduty/aws-guardduty-agent per la violazione delle risorse:::... restrict-image-registries autogen-validate-registries	1. Il cluster Amazon EKS o l'amministratore della sicurezza devono rivedere la politica di sicurezza che blocca l'aggiornamento dell'Addon. 2. È necessario disabilitare il controller (webhook) o fare in modo che il controller accetti le richieste da Amazon EKS.
EKS Addon Issue -ConfigurationConflict : Conflitti rilevati durante il tentativo di candidatura. Non continuerà a causa della modalità di risoluzione dei conflitti. Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.template.spec.containers[name="aws-guardduty-agent"].image	Quando crei o aggiorni l'Addon, fornisci il flag di OVERWRITE risoluzione del conflitto. Ciò potrebbe sovrascrivere qualsiasi modifica apportata direttamente alle risorse correlate in Kubernetes utilizzando l'API Kubernetes. Puoi prima eliminare l'Addon e poi reinstallarlo.

Errore di creazione o aggiornamento del componente aggiuntivo	Fasi per la risoluzione dei problemi
Problema aggiuntivo EKS - `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`	È necessario aggiungere l'autorizzazione mancante al `eks:addon-cluster-admin` `ClusterRoleBinding` manuale. Aggiungi quanto segue `yaml` a`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` `---` Ora puoi applicarlo `yaml` al tuo cluster Amazon EKS utilizzando il seguente comando: `kubectl apply -f eks-addon-cluster-admin.yaml`

Errore di creazione o aggiornamento del componente aggiuntivo	Fasi per la risoluzione dei problemi
Problema relativo al componente aggiuntivo EKS - `AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label`	È necessario disabilitare il controller o fare in modo che il controller accetti le richieste dal cluster Amazon EKS. Prima di creare o aggiornare il componente aggiuntivo, puoi anche creare uno spazio dei GuardDuty nomi ed etichettarlo come. `owner`

Domande frequenti (FAQ)

Indice

- Perché lo stato di copertura della mia risorsa rimane invariato Unhealthy anche dopo aver abilitato il Runtime Monitoring, distribuito il GuardDuty Security Agent e aver soddisfatto tutti i prerequisiti?
- Chi può visualizzare lo stato di copertura in fase di esecuzione di una risorsa che appartiene alla mia Account AWS?

Perché lo stato di copertura della mia risorsa rimane invariato **`Unhealthy`** anche dopo aver abilitato il Runtime Monitoring, distribuito il GuardDuty Security Agent e aver soddisfatto tutti i prerequisiti?

Se hai appena distribuito il GuardDuty security agent (tramite la configurazione automatica dell'agente o manualmente) o hai seguito i passaggi consigliati per risolvere un problema di copertura, potrebbero essere necessari alcuni minuti prima che lo stato della copertura diventi integro. Puoi controllare periodicamente lo stato della copertura o configurare Amazon EventBridge (EventBridge) per ricevere una notifica quando lo stato della copertura cambia.

Chi può visualizzare lo stato di copertura in fase di esecuzione di una risorsa che appartiene alla mia Account AWS?

Come account membro o account autonomo, puoi visualizzare le statistiche di copertura delle risorse associate ai tuoi account. In qualità di account GuardDuty amministratore delegato di

un'organizzazione, puoi visualizzare le statistiche di copertura per le risorse associate al tuo account e gli account dei membri che appartengono alla tua organizzazione.

Configurazione del monitoraggio della CPU e della memoria

Dopo aver abilitato il monitoraggio del runtime e verificato che lo stato di copertura del cluster sia integro, puoi configurare e visualizzare le metriche di analisi.

I seguenti argomenti possono aiutarti a valutare le prestazioni dell'agente distribuito rispetto ai limiti di CPU e memoria dell' GuardDuty agente.

Configurazione del monitoraggio sul cluster Amazon ECS

I seguenti passaggi della Amazon CloudWatch User Guide possono aiutarti a valutare le prestazioni dell'agente distribuito rispetto ai limiti di CPU e memoria per l' GuardDuty agente:

1. Configurazione di Container Insights su Amazon ECS per metriche a livello di cluster e servizio
2. Parametri di Amazon ECS Container Insights

Configurazione del monitoraggio sul cluster Amazon EKS

Dopo aver implementato il GuardDuty security agent e verificato che lo stato di copertura del cluster sia integro, puoi configurare e visualizzare le metriche di Container Insight.

Valuta le prestazioni del security agent

1. Configurazione di Container Insights su Amazon EKS e Kubernetes nella Amazon User Guide CloudWatch
2. Parametri di Amazon EKS e Kubernetes Container Insights nella Amazon User Guide CloudWatch

Gestisci le prestazioni con Security Agent v1.5.0 e versioni successive

Con Security Agent v1.5.0 e versioni successive, quando le informazioni indicano che l' GuardDuty agente associato sta raggiungendo i limiti assegnati, puoi configurare parametri specifici. Per ulteriori informazioni, consulta Configura i parametri aggiuntivi EKS.

Tipi di eventi di runtime raccolti che utilizza GuardDuty

Il GuardDuty security agent raccoglie i seguenti tipi di eventi e li invia al GuardDuty backend per il rilevamento e l'analisi delle minacce. GuardDuty non rende questi eventi accessibili all'utente. Se GuardDuty rileva una potenziale minaccia e genera un risultato di Runtime Monitoring, puoi visualizzare i dettagli del risultato corrispondente. Per ulteriori informazioni su come GuardDuty utilizza i tipi di eventi raccolti, vedereRifiuto esplicito all'utilizzo dei dati volto al miglioramento del servizio.

Eventi di processo

Nome campo	Descrizione
Process name (Nome del processo)	Nome del processo osservato.
Percorso del processo	Percorso assoluto dell'eseguibile del processo.
ID processo	L'ID che il sistema operativo assegna al processo.
PID dello spazio dei nomi	L'ID del processo in uno spazio dei nomi PID secondario diverso dallo spazio dei nomi PID a livello di host. Per i processi all'interno di un container, corrisponde all'ID processo osservabile nel container.
ID utente del processo	L'ID univoco dell'utente che ha eseguito il processo.
UUID processo	L'ID univoco assegnato al processo da GuardDuty.
GID processo	L'ID processo del gruppo di processi.
EGID processo	L'ID di gruppo effettivo del gruppo di processi.
EUID processo	L'ID utente effettivo del processo.
Nome utente del processo	Il nome dell'utente che ha eseguito il processo.

Nome campo	Descrizione
Ora di inizio del processo	L'ora in cui è stato creato il processo. Questo campo è nel formato della stringa di data UTC (`2023-03-22T19:37:20.168Z`).
SHA-256 eseguibile del processo	L'hash `SHA256` dell'eseguibile del processo.
Percorso dello script di processo	Il percorso del file di script che è stato eseguito.
Variabile di ambiente del processo	La variabile di ambiente messa a disposizione del processo. Vengono raccolti solo `LD_PRELOAD` e `LD_LIBRARY_PATH` .
Directory di lavoro presente (PWD) del processo	La directory di lavoro presente del processo.
Processo padre	I dettagli del processo padre. Un processo padre è un processo che ha creato quello osservato.
Argomenti della riga di comando Attualmente, questo campo è limitato a versioni di agenti specifiche corrispondenti al tipo di risorsa: • Fargate (solo Amazon ECS) con GuardDuty security agent v1.0.0 e versioni successive. • Istanze Amazon EC2 con GuardDuty security agent v1.0.0 e versioni successive. • Cluster Amazon EKS con security agent v1.4.0 e versioni successive. Per ulteriori informazioni, consulta GuardDuty cronologia delle versioni degli agenti.	Argomenti della riga di comando forniti al momento dell'esecuzione del processo. Questo campo potrebbe contenere dati sensibili dei clienti.

Eventi del container

Nome campo	Descrizione
Nome container	Il nome del container. Se disponibile, questo campo mostra il valore dell'etichetta `io.kubenetes.container.name` .
UID Container	L'ID univoco del container assegnato dal runtime del container.
Runtime del container	Il runtime del container (ad esempio `docker` o `containerd`) utilizzato per eseguire il container.
ID immagine del container	L'ID dell'immagine del container.
Nome immagine del container	Il nome dell'immagine del container.

AWS Fargate (solo Amazon ECS) eventi relativi alle attività

Nome campo	Descrizione
Nome risorsa Amazon (ARN) dell'attività	L'ARN dell'attività.
Nome del cluster	Il nome del cluster Amazon ECS.
Cognome	Cognome della definizione dell'attività. `family`Viene utilizzato come nome per la definizione dell'attività utilizzata per avviare l'attività.
Nome del servizio	Il nome del servizio Amazon ECS, se l'attività è stata avviata come parte di un servizio.
Tipo di lancio	L'infrastruttura su cui viene eseguita l'attività. Per Runtime Monitoring con tipo di risorsa as`ECSCluster` , il tipo di avvio potrebbe essere uno `EC2` o`FARGATE`.

Nome campo	Descrizione
CPU	Il numero di unità CPU utilizzate dall'attività, espresso nella definizione dell'attività.

Eventi pod di Kubernetes

Nome campo	Descrizione
ID pod	L'ID del pod di Kubernetes.
Nome pod	Il nome del pod di Kubernetes.
Spazio dei nomi pod	Il nome dello spazio dei nomi di Kubernetes a cui appartiene il carico di lavoro di Kubernetes.
Nome del cluster Kubernetes	Il nome del cluster Kubernetes.

Eventi DNS

Nome campo	Descrizione
Tipo di socket	Il tipo di socket per indicare la semantica della comunicazione. Ad esempio, `SOCK_RAW`.
Famiglia di indirizzi	Rappresenta il protocollo di comunicazione associato all'indir izzo. Ad esempio, la famiglia di indirizzi `AF_INET` viene utilizzata per il protocollo IPv4.
ID direzione	L'ID della direzione della connessione.
Numero di protocollo	Il numero di protocollo di livello 4, ad esempio 17 per l'UDP e 6 per il TCP.
IP dell'endpoint remoto DNS	L'IP remoto della connessione.

Nome campo	Descrizione
Porta dell'endpoint remoto DNS	Il numero di porta della connessione.
IP dell'endpoint locale DNS	L'IP locale della connessione.
Porta dell'endpoint locale DNS	Il numero di porta della connessione.
Payload DNS	Il payload di pacchetti DNS che contiene query e risposte DNS.

Eventi aperti

Nome campo	Descrizione
Percorso del file	Il percorso del file aperto in questo evento.
Flag	Descrive la modalità di accesso ai file, ad esempio sola lettura, sola scrittura e lettura e scrittura.

Evento modulo di caricamento

Nome campo	Descrizione
Nome del modulo	Il nome del modulo caricato nel kernel.

Eventi mprotect

Nome campo	Descrizione
Intervallo di indirizzi	L'intervallo di indirizzi per il quale sono state modificate le protezioni di accesso.
Regioni di memoria	Specifica la regione dello spazio degli indirizzi di un processo, ad esempio stack e heap.

Nome campo	Descrizione
Flag	Rappresenta le opzioni che controllano il comportamento di questo evento.

Eventi di montaggio

Nome campo	Descrizione
Destinazione di montaggio	Il percorso in cui è montata l'origine di montaggio.
Origine di montaggio	Il percorso sull'host montato sulla destinazione di montaggio.
Tipo di file system	Rappresenta il tipo di file system montato.
Flag	Rappresenta le opzioni che controllano il comportamento di questo evento.

Eventi di collegamento

Nome campo	Descrizione
Percorso di collegamento	Il percorso in cui viene creato il collegamento fisico.
Percorso di destinazione	Il percorso del file a cui punta il collegamento fisico.

Eventi collegamento simbolico

Nome campo	Descrizione
Percorso di collegamento	Il percorso in cui viene creato il collegamento simbolico.
Percorso di destinazione	Il percorso del file a cui punta il collegamento simbolico.

Eventi dup

Nome campo	Descrizione
Vecchio descrittore di file	Un descrittore di file che rappresenta un oggetto file aperto.
Nuovo descrittore di file	Un nuovo descrittore di file che è un duplicato di quello vecchio. Sia il descrittore di file vecchio che quello nuovo rappresentano lo stesso oggetto file aperto.
IP dell'endpoint remoto dup	L'indirizzo IP remoto del socket di rete rappresentato dal vecchio descrittore di file. Applicabile solo quando il vecchio descrittore di file rappresenta un socket di rete.
Porta dell'endpoint remoto dup	La porta remota del socket di rete rappresentato dal vecchio descrittore di file. Applicabile solo quando il vecchio descrittore di file rappresenta un socket di rete.
IP dell'endpoint locale dup	L'indirizzo IP locale del socket di rete rappresentato dal vecchio descrittore di file. Applicabile solo quando il vecchio descrittore di file rappresenta un socket di rete.
Porta dell'endpoint locale dup	La porta locale del socket di rete rappresentato dal vecchio descrittore di file. Applicabile solo quando il vecchio descrittore di file rappresenta un socket di rete.

Evento mappa di memoria

Nome campo	Descrizione
Percorso del file	Il percorso del file su cui la memoria viene mappata.

Eventi socket

Nome campo	Descrizione
Famiglia di indirizzi	Rappresenta il protocollo di comunicazione associato all'indirizzo. Ad esempio, la famiglia di indirizzi `AF_INET` viene utilizzata per la versione IP del protocollo 4.
Tipo di socket	Il tipo di socket per indicare la semantica della comunicazione. Ad esempio, `SOCK_RAW`.
Numero di protocollo	Specifica un protocollo particolare all'interno della famiglia di indirizzi. In genere esiste un unico protocollo nelle famiglie di indirizzi. Ad esempio, la famiglia di indirizzi `AF_INET` ha solo il protocollo IP.

Connetti eventi

Nome campo	Descrizione
Famiglia di indirizzi	Rappresenta il protocollo di comunicazione associato all'indirizzo. Ad esempio, la famiglia di indirizzi `AF_INET` viene utilizzata per il protocollo IPv4.
Tipo di socket	Il tipo di socket per indicare la semantica della comunicazione. Ad esempio, `SOCK_RAW`.
Numero di protocollo	Specifica un protocollo particolare all'interno della famiglia di indirizzi. In genere esiste un unico protocollo nelle famiglie di indirizzi. Ad esempio, la famiglia di indirizzi `AF_INET` ha solo il protocollo IP.
Percorso del file	Il percorso del file socket se la famiglia di indirizzi è `AF_UNIX`.
IP dell'endpoint remoto	L'IP remoto della connessione.
Porta dell'endpoint remoto	Il numero di porta della connessione.

Nome campo	Descrizione
IP dell'endpoint locale	L'IP locale della connessione.
Porta dell'endpoint locale	Il numero di porta della connessione.

Eventi VM Readv processo

Nome campo	Descrizione
Flag	Rappresenta le opzioni che controllano il comportamento di questo evento.
PID di destinazione	L'ID processo del processo da cui viene letta la memoria.
UUID del processo di destinazione	L'ID univoco del processo di destinazione.
Percorso eseguibile di destinazione	Il percorso assoluto del file eseguibile del processo di destinazione.

Eventi VM Writev processo

Nome campo	Descrizione
Flag	Rappresenta le opzioni che controllano il comportamento di questo evento.
PID di destinazione	L'ID processo del processo su cui viene scritta la memoria.
UUID del processo di destinazione	L'ID univoco del processo di destinazione.
Percorso eseguibile di destinazione	Il percorso assoluto del file eseguibile del processo di destinazione.

Eventi ptrace

Nome campo	Descrizione
PID di destinazione	L'ID processo del processo di destinazione.
UUID del processo di destinazione	L'ID univoco del processo di destinazione.
Percorso eseguibile di destinazione	Il percorso assoluto del file eseguibile del processo di destinazione.
Flag	Rappresenta le opzioni che controllano il comportamento di questo evento.

Associa eventi

Nome campo	Descrizione
Famiglia di indirizzi	Rappresenta il protocollo di comunicazione associato all'indirizzo. Ad esempio, la famiglia di indirizzi `AF_INET` viene utilizzata per il protocollo IPv4.
Tipo di socket	Il tipo di socket per indicare la semantica della comunicazione. Ad esempio, `SOCK_RAW`.
Numero di protocollo	Il numero di protocollo di livello 4, ad esempio 17 per l'UDP e 6 per il TCP.
IP dell'endpoint locale	L'IP locale della connessione.
Porta endpoint locale	Il numero di porta della connessione.

Ascolta gli eventi

Nome campo	Descrizione
Famiglia di indirizzi	Rappresenta il protocollo di comunicazione associato all'indirizzo. Ad esempio, la famiglia di indirizzi `AF_INET` viene utilizzata per il protocollo IPv4.
Tipo di socket	Il tipo di socket per indicare la semantica della comunicazione. Ad esempio, `SOCK_RAW`.
Numero di protocollo	Il numero di protocollo di livello 4, ad esempio 17 per l'UDP e 6 per il TCP.
IP dell'endpoint locale	L'IP locale della connessione.
Porta endpoint locale	Il numero di porta della connessione.

Rinomina gli eventi

Nome campo	Descrizione
Percorso del file	Percorso in cui si trova il file che viene rinominato.
Target	Il nuovo percorso del file.

Imposta gli eventi UID

Nome campo	Descrizione
Nuovo EUID	Il nuovo ID utente effettivo del processo.
Nuovo UID	Il nuovo ID utente del processo.

Eventi Chmod

Nome campo	Descrizione
Percorso del file	Percorso del file che richiama questo evento.
Modalità file	Le autorizzazioni di accesso aggiornate per il file associato.

Agente di hosting del repository Amazon ECR GuardDuty

Nelle sezioni seguenti sono elencati i repository Amazon Elastic Container Registry (Amazon ECR) GuardDuty in cui è ospitato l'agente di sicurezza che viene distribuito sui cluster Amazon EKS e Amazon ECS.

Indice

- Repository per GuardDuty agenti su cluster Amazon EKS
- Repository per GuardDuty agente su AWS Fargate (solo Amazon ECS)

Repository per GuardDuty agenti su cluster Amazon EKS

La tabella seguente mostra i repository Amazon ECR che ospitano l'agente aggiuntivo Amazon EKS per GuardDuty (`aws-guardduty-agent`) per ciascuno. Regione AWS

Regione AWS	URI del repository Amazon ECR
US West (Oregon)	`039403964562.dkr.ecr.us-west-2.amazonaws.com`
Europa (Parigi)	`113643092156.dkr.ecr.eu-west-3.amazonaws.com`
Asia Pacifico (Mumbai)	`610108029387.dkr.ecr.ap-south-1.amazonaws.com`
Asia Pacific (Hyderabad)	`618745550137.dkr.ecr.ap-south-2.amazonaws.com`

Regione AWS	URI del repository Amazon ECR
Canada (Centrale)	`001188825231.dkr.ecr.ca-central-1.amazonaws.com`
Medio Oriente (Emirati Arabi Uniti)	`601769779514.dkr.ecr.me-central-1.amazonaws.com`
Europa (Londra)	`109118265657.dkr.ecr.eu-west-2.amazonaws.com`
Europa (Irlanda)	`373421517865.dkr.ecr.us-west-1.amazonaws.com`
Stati Uniti orientali (Virginia settentrionale)	`031903291036.dkr.ecr.us-east-1.amazonaws.com`
Stati Uniti orientali (Ohio)	`591382732059.dkr.ecr.us-east-2.amazonaws.com`
Europa (Irlanda)	`673884943994.dkr.ecr.eu-west-1.amazonaws.com`
Sud America (San Paolo)	`941219317354.dkr.ecr.sa-east-1.amazonaws.com`
Europa (Stoccolma)	`366771026645.dkr.ecr.eu-north-1.amazonaws.com`
Europa (Francoforte)	`409493279830.dkr.ecr.eu-central-1.amazonaws.com`
Europa (Zurigo)	`718440343717.dkr.ecr.eu-central-2.amazonaws.com`
Asia Pacifico (Singapore)	`584580519942.dkr.ecr.ap-southeast-1.amazonaws.com`
Asia Pacifico (Sydney)	`011662287384.dkr.ecr.ap-southeast-2.amazonaws.com`

Regione AWS	URI del repository Amazon ECR
Asia Pacifico (Giacarta)	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
Asia Pacifico (Tokyo)	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
Asia Pacifico (Seul)	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asia Pacifico (Osaka-Locale)	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Asia Pacifico (Hong Kong)	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Medio Oriente (Bahrein)	541829937850.dkr.ecr.me-south-1.amazonaws.com
Europa (Milano)	528450769569.dkr.ecr.eu-south-1.amazonaws.com
Europa (Spagna)	531047660167.dkr.ecr.eu-south-2.amazonaws.com
Africa (Città del Capo)	379032919888.dkr.ecr.af-south-1.amazonaws.com
Asia Pacifico (Melbourne)	750462861327.dkr.ecr.ap-southeast-4.amazonaws.com
Israele (Tel Aviv)	292660727137.dkr.ecr.il-central-1.amazonaws.com

Repository per GuardDuty agente su AWS Fargate (solo Amazon ECS)

La tabella seguente mostra i repository Amazon ECR che ospitano l' GuardDuty agente per (solo AWS Fargate Amazon ECS) per ciascuno di essi. Regione AWS

Regione AWS	URI del repository Amazon ECR
US West (Oregon)	733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-fargate
Europa (Parigi)	665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Mumbai)	251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacific (Hyderabad)	950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guardduty-agent-fargate
Canada (Centrale)	354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-fargate
Medio Oriente (Emirati Arabi Uniti)	000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Londra)	892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-fargate
Europa (Irlanda)	684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-fargate
Stati Uniti orientali (Virginia settentrionale)	593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-fargate
Stati Uniti orientali (Ohio)	307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-fargate
Europa (Irlanda)	694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-fargate
Sud America (San Paolo)	758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-fargate

Regione AWS	URI del repository Amazon ECR
Europa (Stoccolma)	591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Francoforte)	323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Zurigo)	529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Singapore)	174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Sydney)	005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Giacarta)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Tokyo)	533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Seul)	914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Osaka-Locale)	273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Hong Kong)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate
Medio Oriente (Bahrein)	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Milano)	266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Spagna)	919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate

Regione AWS	URI del repository Amazon ECR
Africa (Città del Capo)	`197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Asia Pacifico (Melbourne)	`251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate`
Israele (Tel Aviv)	`870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate`

GuardDuty cronologia delle versioni degli agenti

Le seguenti sezioni forniscono la versione di rilascio per l' GuardDuty agente che viene distribuito su istanze Amazon EC2, cluster Amazon ECS e cluster Amazon EKS.

GuardDuty agente di sicurezza per istanze Amazon EC2

Versione agente	Note di rilascio	Data di disponibilità
v1.1.0	Supporta la configurazione GuardDuty automatizzata degli agenti in Runtime Monitoring per le istanze Amazon EC2. Supporta nuovi segnali e risultati di sicurezza rilasciati con l'annuncio della disponibi lità generale di Runtime Monitoring per le istanze EC2. Miglioramento generale delle prestazioni.	26 marzo 2024
v1.0.2	Supporta le AMI Amazon ECS più recenti.	2 febbraio 2024

Versione agente	Note di rilascio	Data di disponibilità
v1.0.1	Ottimizzazione e miglioramenti generali delle prestazioni Le versioni degli agenti rilasciate prima della v1.0.2 sono incompatibili con le AMI Amazon ECS lanciate dopo il 31 gennaio 2024.	23 gennaio 2024
v1.0.0	Versione iniziale dell'inst allazione RPM. Le versioni degli agenti rilasciate prima della v1.0.2 sono incompatibili con le AMI Amazon ECS lanciate dopo il 31 gennaio 2024.	26 novembre 2023

La chiave pubblica, la firma di x86_64 RPM, la firma di arm64 RPM e il collegamento di accesso corrispondente agli script RPM ospitati nei bucket Amazon S3 possono essere formati dai seguenti modelli. Sostituisci il valore dell'ID dell' AWS account e la versione dell' Regione AWS agente per accedere agli script RPM. GuardDuty I seguenti modelli includono l'ultima versione dell'agente per le istanze Amazon EC2.

- Chiave pubblica:

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/publickey.pem
```

- GuardDuty firma RPM dell'agente di sicurezza:

  Firma di x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/amazon-guardduty-agent-1.1.0.x86_64.sig
```

Firma di arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/amazon-guardduty-agent-1.1.0.arm64.sig
```

- Accedi ai link agli script RPM nel bucket Amazon S3:

  Link di accesso per x86_64 RPM

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/amazon-guardduty-agent-1.1.0.x86_64.rpm
  ```

  Link di accesso per arm64 RPM

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/amazon-guardduty-agent-1.1.0.arm64.rpm
  ```

Regione AWS	Nome Regione	AWS ID dell'account
eu-west-1	Europa (Irlanda)	694911143906
us-east-1	Stati Uniti orientali (Virginia settentrionale)	593207742271
us-east-2	Stati Uniti orientali (Ohio)	733349766148
eu-west-3	Europa (Parigi)	665651866788
us-east-2	Stati Uniti orientali (Ohio)	307168627858
eu-central-1	Europa (Francoforte)	323658145986
ap-northeast-2	Asia Pacifico (Seul)	914738172881
eu-north-1	Europa (Stoccolma)	591436053604
ap-east-1	Asia Pacifico (Hong Kong)	258348409381
me-south-1	Medio Oriente (Bahrein)	536382113932

eu-west-2	Europa (Londra)	892757235363
ap-northeast-1	Asia Pacifico (Tokyo)	533107202818
ap-southeast-1	Asia Pacifico (Singapore)	174946120834
ap-south-1	Asia Pacifico (Mumbai)	251508486986
ap-southeast-3	Asia Pacifico (Giacarta)	510637619217
sa-east-1	Sud America (San Paolo)	758426053663
ap-northeast-3	Asia Pacifico (Osaka-Locale)	273192626886
eu-south-1	Europa (Milano)	266869475730
af-south-1	Africa (Città del Capo)	197869348890
ap-southeast-2	Asia Pacifico (Sydney)	005257825471
me-central-1	Medio Oriente (Emirati Arabi Uniti)	000014521398
us-west-1	Stati Uniti occidentali (California settentrionale)	684579721401
ca-central-1	Canada (Centrale)	354763396469
ap-south-2	Asia Pacific (Hyderabad)	950823858135
eu-south-2	Europa (Spagna)	919611009337
eu-central-2	Europa (Zurigo)	529164026651
ap-southeast-4	Asia Pacifico (Melbourne)	251357961535
il-central-1	Israele (Tel Aviv)	870907303882

GuardDuty agente di sicurezza per AWS Fargate (solo Amazon ECS)

La tabella seguente mostra la cronologia delle versioni di rilascio del GuardDuty Security Agent per Fargate (solo Amazon ECS).

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità
v1.0.0	x86_64 (AMD64): `sha256:359b8b014e5076c625daa1056090e522631587a7afa3b2e055edda6bd1141017` Graviton (ARM64): `sha256:b9438690fa8a86067180a11658bec0f4f838ae3fbd225d04b9306250648b3984`	Versione iniziale di GuardDuty Security Agent per AWS Fargate (solo Amazon ECS).	26 novembre 2023

GuardDuty agente di sicurezza per cluster Amazon EKS

La tabella seguente mostra la cronologia delle versioni di rilascio dell' GuardDuty agente aggiuntivo Amazon EKS.

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità	Fine del supporto standard 1
v1.5.0	x86_64 (AMD64): `sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c` Graviton (ARM64): `sha256:537a330b2dd82357024fb6daeb876`	• Ottimizzazione e miglioramenti generali delle prestazioni.	07 marzo 2024	–

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità	Fine del supporto standard 1
	`1034b7defd43b10dffe0792c9e6d0778b40`	• Miglioramenti della sicurezza, inclusi nuovi tipi di eventi in. Tipi di eventi di runtime raccolti • Miglioramenti delle prestazioni relativi all'utilizzo della CPU.		
v1.4.1	x86_64 (AMD64): `sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c` Graviton (ARM64): `sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dffe0792c9e6d0778b40`	Ottimizzazione e miglioramenti generali delle prestazioni.	16 gennaio 2024	–

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità	Fine del supporto standard 1
v1.4.0	x86_64 (AMD64): `sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f` Graviton (ARM64): `sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e`	Il punto di montaggio Manifest supporta una migliore raccolta dei dati AppArmor configurazione in manifest Raccogli l'argomento della riga di comando Ottimizzazione e miglioramenti generali delle prestazioni	21 dicembre 2023	–
v1.3.1	x86_64 (AMD64): `sha256:55578fcb7b73097ade5c8404390ef16cf76a7b568490abaae01ac75992b3ea29` Graviton (ARM64): `sha256:e3ce8d66ac2121f8d476eb58f8bc50ab51336647615eb7cf514c21421cb818fd`	Patch di sicurezza e aggiornamenti importanti.	23 ottobre 2023	–

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità	Fine del supporto standard 1
v1.3.0	x86_64 (AMD64): `sha256:6dace2337dfbb7609811be89fb4b23ae0b865f1027ad78fbe69530bfbd46c694` Graviton (ARM64): `sha256:4928a7c6ef40e77c8ec95841323bb9a110db31f12c0ee7ab965e08b43efd01bb`	Supporta la piattaforma Ubuntu Supporta la versione 1.28 di Kubernetes Miglioramenti generali delle prestazioni e miglioramento della stabilità.	5 ottobre 2023	–

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità	Fine del supporto standard 1
v1.2.0	x86_64 (AMD64): `sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3` Graviton (ARM64): `sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa`	Oltre alle istanze basate su AMD64, ora la versione 1.2.0 supporta anche quelle basate su ARM64. È stato aggiunto e verificato il supporto per Bottlerocket Supporta la versione 1.27 di Kubernetes Miglioramenti generali delle prestazioni e miglioramenti della stabilità.	16 giugno 2023	–

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità	Fine del supporto standard [1]
v1.1.0	`sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c`	Oltre a Versioni di Kubernetes supportate dal security agent GuardDuty, questa versione dell'agente supporta anche la versione 1.26 di Kubernetes. Miglioramenti generali delle prestazioni e miglioramenti della stabilità.	2 maggio 2023	14 maggio 2024
v1.0.0	`sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e`	Versione iniziale dell'agente (componente aggiuntivo di Amazon EKS).	30 marzo 2023	14 maggio 2024

- [1] Per informazioni sull'aggiornamento della versione corrente dell'agente che si avvicina alla fine del supporto standard, consulta. Aggiornamento manuale del security agent

Protezione Amazon S3 su Amazon GuardDuty

S3 Protection aiuta Amazon a GuardDuty monitorare gli eventi AWS CloudTrail relativi ai dati per Amazon Simple Storage Service (Amazon S3) che includono operazioni API a livello di oggetto per identificare potenziali rischi per la sicurezza dei dati all'interno dei bucket Amazon S3.

GuardDuty monitora sia gli eventi di AWS CloudTrail gestione che gli eventi relativi ai dati AWS CloudTrail S3 per identificare potenziali minacce nelle tue risorse Amazon S3. Le due origini dati monitorano diversi tipi di attività. Esempi di eventi di CloudTrail gestione per S3 includono operazioni che elencano o configurano i bucket Amazon S3, `ListBuckets` come`DeleteBuckets`, e. `PutBucketReplication` Esempi di eventi CloudTrail relativi ai dati per S3 includono operazioni API a livello di oggetto, come,, e. `GetObject` `ListObjects` `DeleteObject` `PutObject`

Quando abiliti Amazon GuardDuty for an Account AWS, GuardDuty inizia a monitorare gli eventi CloudTrail di gestione. Non è necessario abilitare o configurare manualmente la registrazione degli eventi relativi ai dati S3. AWS CloudTrail Puoi abilitare la funzionalità S3 Protection (che monitora gli eventi CloudTrail relativi ai dati per S3) per qualsiasi account in qualsiasi Regione AWS luogo in cui questa funzionalità è disponibile in Amazon GuardDuty, in qualsiasi momento. Se è Account AWS già abilitata GuardDuty, puoi abilitare S3 Protection per la prima volta con un periodo di prova gratuito di 30 giorni. Per una versione Account AWS che viene abilitata GuardDuty per la prima volta, S3 Protection è già abilitata e inclusa in questa prova gratuita di 30 giorni. Per ulteriori informazioni, consulta Stima dei costi GuardDuty .

Ti consigliamo di abilitare S3 Protection in. GuardDuty Se questa funzionalità non è abilitata, non GuardDuty sarà possibile monitorare completamente i bucket Amazon S3 o generare rilevazioni di accessi sospetti ai dati archiviati nei bucket S3.

Come vengono utilizzati gli eventi relativi ai dati di S3 GuardDuty

Quando abiliti gli eventi relativi ai dati S3 (S3 Protection), GuardDuty inizia ad analizzare gli eventi relativi ai dati S3 provenienti da tutti i bucket S3 e li monitora per rilevare eventuali attività dannose e sospette. Per ulteriori informazioni, consulta AWS CloudTrail eventi relativi ai dati per S3.

Quando un utente non autenticato accede a un oggetto S3, significa che l'oggetto S3 è accessibile pubblicamente. Pertanto, GuardDuty non elabora tali richieste. GuardDuty elabora le richieste fatte agli oggetti S3 utilizzando credenziali IAM (AWS Identity and Access Management) o AWS STS (AWS Security Token Service) valide.

Quando GuardDuty rileva una potenziale minaccia basata sul monitoraggio degli eventi relativi ai dati di S3, genera un risultato di sicurezza. Per informazioni sui tipi di risultati che è GuardDuty possibile generare per i bucket Amazon S3, consulta. GuardDuty Tipi di ricerca S3

Se disabiliti S3 Protection, GuardDuty interrompe il monitoraggio degli eventi relativi ai dati archiviati nei bucket S3 di S3.

Configurazione della Protezione S3 per un account autonomo

Per gli account associati da AWS Organizations, questo processo può essere automatizzato tramite le impostazioni della console. Per ulteriori informazioni, consulta Configurazione della Protezione S3 in ambienti con più account.

Per abilitare o disabilitare la Protezione S3

Scegli il metodo di accesso che preferisci per configurare la Protezione S3 per un account autonomo.

Console

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Protezione S3.
3. La pagina Protezione S3 fornisce lo stato attuale della Protezione S3 per il tuo account. Scegli Abilita o Disabilita per abilitare o disabilitare in qualsiasi momento la Protezione S3.
4. Scegli Conferma per confermare la selezione.

API/CLI

1. Esegui updateDetector utilizzando l'ID rilevatore valido per la regione attuale e impostando il `name` dell'oggetto `features` da `S3_DATA_EVENTS` a `ENABLED` o `DISABLED` rispettivamente per abilitare o disabilitare la Protezione S3.

> **Note**
>
> Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

2. In alternativa, puoi usare AWS Command Line Interface. Per abilitare la Protezione S3, esegui il comando seguente e assicurati di utilizzare il tuo ID rilevatore valido.

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

   Per disabilitare la Protezione S3, sostituisci `ENABLED` con `DISABLED` nell'esempio.

Configurazione della Protezione S3 in ambienti con più account

In un ambiente con più account, solo l'account GuardDuty amministratore delegato ha la possibilità di configurare (abilitare o disabilitare) S3 Protection per gli account dei membri della propria organizzazione. AWS GuardDuty Gli account membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce i propri account membro utilizzando AWS Organizations. L'account GuardDuty amministratore delegato può scegliere di abilitare automaticamente S3 Protection su tutti gli account, solo sui nuovi account o su nessun account dell'organizzazione. Per ulteriori informazioni, consulta Gestione degli account con AWS Organizations.

Configurazione di S3 Protection per l'account amministratore delegato GuardDuty

Scegli il metodo di accesso preferito per configurare S3 Protection per l'account amministratore delegato. GuardDuty

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali dell'account di gestione.
2. Nel riquadro di navigazione, scegli Protezione S3.
3. Nella pagina Protezione S3, scegli Modifica.
4. Esegui una di queste operazioni:

   Utilizzando Abilita per tutti gli account

   - Scegli Abilita per tutti gli account. Ciò abiliterà il piano di protezione per tutti gli GuardDuty account attivi AWS dell'organizzazione, inclusi i nuovi account che entrano a far parte dell'organizzazione.

- Selezionare Salva.

Utilizzando Configura gli account manualmente

- Per abilitare il piano di protezione solo per l'account GuardDuty amministratore delegato, scegli Configura gli account manualmente.
- Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).
- Selezionare Salva.

API/CLI

Esegui updateDetectorutilizzando l'ID del rilevatore dell'account GuardDuty amministratore delegato per la regione corrente e passando l'`features`oggetto `name` come `S3_DATA_EVENTS` e `status` come o. `ENABLED` `DISABLED`

In alternativa, puoi configurare S3 Protection utilizzando. AWS Command Line Interface*Esegui il comando seguente e assicurati di sostituire 12abc34d567e8fa901bc2d34e56789f0 con l'ID del rilevatore dell'account amministratore delegato per la regione corrente e 5555 con l'ID dell'account amministratore delegato. GuardDuty* Account AWS GuardDuty

Per trovare il codice per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/. **`detectorId`**

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 555555555555 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

Abilitare automaticamente la Protezione S3 per tutti gli account membri dell'organizzazione

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando il tuo account amministratore.
2. Esegui una di queste operazioni:

Utilizzando la pagina Protezione S3

1. Nel riquadro di navigazione, scegli Protezione S3.
2. Scegli Abilita per tutti gli account. Questa operazione abilita automaticamente la Protezione S3 per gli account dell'organizzazione esistenti e per quelli nuovi.
3. Selezionare Salva.

> **Note**
>
> L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Utilizzando la pagina Account

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
3. Nella finestra Gestisci le preferenze di abilitazione automatica, scegli Abilita per tutti gli account in Protezione S3.
4. Selezionare Salva.

Se non puoi utilizzare l'opzione Abilita per tutti gli account, consulta Abilitare o disabilitare in modo selettivo la Protezione S3 negli account membri.

API/CLI

- Per abilitare o disabilitare in modo selettivo la Protezione S3 per i tuoi account membri, richiama l'operazione API updateMemberDetectors utilizzando il tuo *ID rilevatore*.
- L'esempio seguente mostra come abilitare la Protezione S3 per un singolo account membro. *Assicurati di sostituire 12abc34d567e8fa901bc2d34e56789f0 con l'account amministratore delegato e 111122223333. detector-id GuardDuty* Per disabilitare la Protezione S3, sostituisci `ENABLED` con `DISABLED`.

  Per trovare `detectorId` le informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

> **Note**
>
> Puoi anche trasmettere un elenco di ID account separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare la Protezione S3 per tutti gli account membri attivi esistenti

Scegli il metodo di accesso che preferisci per abilitare la Protezione S3 per tutti gli account membri attivi esistenti dell'organizzazione.

Console

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.
2. Nel riquadro di navigazione, scegli Protezione S3.
3. Nella pagina Protezione S3, puoi visualizzare lo stato attuale della configurazione. Nella sezione Account membri attivi, scegli Operazioni.
4. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
5. Scegli Conferma.

API/CLI

- Per abilitare o disabilitare in modo selettivo la Protezione S3 per i tuoi account membri, richiama l'operazione API updateMemberDetectors utilizzando il tuo *ID rilevatore*.
- L'esempio seguente mostra come abilitare la Protezione S3 per un singolo account membro. *Assicurati di sostituire 12abc34d567e8fa901bc2d34e56789f0 con*

l'account dell'amministratore delegato e 111122223333. detector-id GuardDuty Per disabilitare la Protezione S3, sostituisci `ENABLED` con `DISABLED`.

Per trovare `detectorId` le informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

> **Note**
>
> Puoi anche trasmettere un elenco di ID account separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare automaticamente la Protezione S3 per i nuovi account membri

Scegli il metodo di accesso che preferisci per abilitare la Protezione S3 per i nuovi account che entrano a far parte dell'organizzazione.

Console

L'account GuardDuty amministratore delegato può abilitare nuovi account membro in un'organizzazione tramite la console, utilizzando la pagina Protezione S3 o Account.

Per abilitare automaticamente la Protezione S3 per i nuovi account membri

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.
2. Esegui una di queste operazioni:
   - Utilizzando la pagina Protezione S3:

     1. Nel riquadro di navigazione, scegli Protezione S3.
     2. Nella pagina Protezione S3, scegli Modifica.

3. Scegli Configura gli account manualmente.
4. Seleziona Abilita automaticamente per i nuovi account membri. Questa fase garantisce l'abilitazione automatica della Protezione S3 per ogni nuovo account che entra a far parte dell'organizzazione. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa configurazione.
5. Selezionare Salva.

- Utilizzando la pagina Account:

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica.
3. Nella finestra Gestisci le preferenze di abilitazione automatica, seleziona Abilita per nuovi account in Protezione S3.
4. Selezionare Salva.

API/CLI

- Per abilitare o disabilitare in modo selettivo la Protezione S3 per i tuoi account membri, richiama l'operazione API UpdateOrganizationConfiguration utilizzando il tuo *ID rilevatore*.
- L'esempio seguente mostra come abilitare la Protezione S3 per un singolo account membro. Per disabilitarla, consulta Abilitare o disabilitare in modo selettivo la Protezione RDS per gli account membri. Imposta le preferenze in modo da abilitare o disabilitare automaticamente il piano di protezione in una determinata regione per i nuovi account che entrano a far parte dell'organizzazione (`NEW`), per tutti gli account (`ALL`) o per nessuno degli account dell'organizzazione (`NONE`). Per ulteriori informazioni, vedere autoEnableOrganizationMembri. In base alle tue preferenze, potrebbe essere necessario sostituire `NEW` con `ALL` o `NONE`.

  Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

> **Note**
>
> Puoi anche trasmettere un elenco di ID account separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare o disabilitare in modo selettivo la Protezione S3 negli account membri

Scegli il metodo di accesso che preferisci per abilitare o disabilitare in modo selettivo la Protezione S3 per gli account membri.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.
2. Dal riquadro di navigazione, selezionare Accounts (Account).

   Nella pagina Account, consulta la colonna Protezione S3 per visualizzare lo stato del tuo account membro.
3. Per abilitare o disabilitare in modo selettivo la Protezione S3

   Seleziona l'account per il quale desideri configurare la Protezione S3. Puoi selezionare più account alla volta. Nel menu a discesa Modifica piani di protezione, scegli S3Pro, quindi scegli l'opzione appropriata.

API/CLI

Per abilitare o disabilitare in modo selettivo la Protezione S3 per i tuoi account membri, esegui l'operazione API updateMemberDetectors utilizzando il tuo ID rilevatore. L'esempio seguente mostra come abilitare la Protezione S3 per un singolo account membro. Per disabilitarla, sostituisci `true` con `false`.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

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

> **Note**
>
> Puoi anche trasmettere un elenco di ID account separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

> **Note**
>
> Se utilizzi script per aggiungere nuovi account nei quali desideri disabilitare la Protezione S3, puoi modificare l'operazione API createDetector con l'oggetto `dataSources` facoltativo, come descritto in questo argomento.

Disattivazione automatica di S3 Protection per i nuovi account GuardDuty

> **Important**
>
> Per impostazione predefinita, S3 Protection è abilitata automaticamente per Account AWS quel join GuardDuty per la prima volta.

Se sei un account GuardDuty amministratore che abilita GuardDuty per la prima volta un nuovo account e non desideri che S3 Protection sia abilitato per impostazione predefinita, puoi disabilitarlo modificando il funzionamento dell'createDetectorAPI con l'oggetto opzionale. `features` L'esempio seguente utilizza AWS CLI per abilitare un nuovo GuardDuty rilevatore con la protezione S3 disabilitata.

```
aws guardduty create-detector --enable --features '[{"Name" : "S3_DATA_EVENTS",
"Status" : "DISABLED"}]'
```

Funzionalità della Protezione S3

AWS CloudTrail eventi relativi ai dati per S3

Gli eventi di dati, anche conosciuti come operazioni del piano dati, forniscono informazioni dettagliate sulle operazioni eseguite su una risorsa o al suo interno e sono spesso attività che interessano volumi elevati di dati.

Di seguito sono riportati alcuni esempi di eventi CloudTrail relativi ai dati per S3 che è GuardDuty possibile monitorare:

- Operazioni API `GetObject`
- Operazioni API `PutObject`
- Operazioni API `ListObjects`
- Operazioni API `DeleteObject`

Quando lo abiliti GuardDuty per la prima volta, S3 Protection è abilitato per impostazione predefinita ed è incluso anche nel periodo di prova gratuito di 30 giorni. Tuttavia, questa funzionalità è facoltativa e puoi scegliere di abilitarla o disabilitarla in qualsiasi momento e per qualsiasi account o regione. Per ulteriori informazioni sulla configurazione della funzionalità di Amazon S3, consulta GuardDuty Protezione S3.

Comprendere i GuardDuty risultati di Amazon

Una GuardDuty scoperta rappresenta un potenziale problema di sicurezza rilevato all'interno della rete. GuardDutygenera un risultato ogni volta che rileva attività impreviste e potenzialmente dannose nell' AWS ambiente in uso.

È possibile visualizzare e gestire i GuardDuty risultati nella pagina Findings della GuardDuty console o utilizzando le operazioni AWS CLI o l'API. Per una panoramica dei modi in cui puoi gestire gli esiti, consulta Gestione dei GuardDuty risultati di Amazon.

Argomenti:

Dettagli degli esiti

Scopri i tipi di dati disponibili all'interno dei GuardDuty risultati.

Risultati di esempio

Scopri come generare risultati di esempio da testare o comprendere meglio GuardDuty.

Formato degli esiti di GuardDuty

Comprendi il formato dei tipi di GuardDuty ricerca e i diversi scopi delle minacce seguiti GuardDuty.

Tipi di esiti

Visualizza e cerca tutti i GuardDuty risultati disponibili per tipo. Ogni voce del tipo di esito include una spiegazione di tale esito, nonché consigli e suggerimenti per la correzione.

Dettagli degli esiti

Nella GuardDuty console Amazon, puoi visualizzare i dettagli della ricerca nella sezione di riepilogo dei risultati. I dettagli degli esiti variano in base al tipo di esito.

Esistono due dettagli principali che determinano il tipo di informazioni disponibili per qualsiasi esito. Il primo è il tipo di risorsa, che può essere `Instance`, `AccessKey`, `S3Bucket`, `Kubernetes cluster`, `ECS cluster`, `Container`, `RDSDBInstance` o `Lambda`. Il secondo dettaglio che determina le informazioni sull'esito è Ruolo risorsa. Il ruolo risorsa può essere `Target` per le

chiavi di accesso, che indica che la risorsa è stata la destinazione di attività sospette. Per gli esiti del tipo istanza, il ruolo risorsa può anche essere `Actor`, che indica che la risorsa è stata l'attore che svolgeva attività sospette. In questo argomento vengono descritti alcuni dei dettagli degli esiti comunemente disponibili.

Panoramica degli esiti

La sezione Panoramica di un esito ne contiene le caratteristiche identificative di base, incluse le informazioni seguenti:

- ID account: l'ID dell' AWS account in cui si è svolta l'attività che ha richiesto la generazione GuardDuty di questo risultato.
- Conteggio: il numero di volte in cui GuardDuty è stata aggregata un'attività che corrisponde a questo schema a questo risultato ID.
- Ora creazione: la data e l'ora di creazione di questo esito. Se questo valore è diverso da Ora aggiornamento significa che l'attività si è verificata più volte e si tratta di un problema in corso.

> **Note**
>
> I timestamp per i risultati nella GuardDuty console vengono visualizzati nel fuso orario locale, mentre le esportazioni JSON e gli output CLI visualizzano i timestamp in UTC.

- ID risultato: un identificatore univoco per questo tipo di esito e insieme di parametri. Le nuove occorrenze di attività corrispondenti a questo modello verranno aggregate allo stesso ID.
- Tipo di esito: una stringa formattata che rappresenta il tipo di attività che ha attivato l'esito. Per ulteriori informazioni, consulta Formato degli esiti di GuardDuty.
- Regione: la regione in cui è stato generato il risultato. AWS Per ulteriori informazioni sulle regioni supportate, consulta Regioni ed endpoint.
- ID risorsa: l'ID della AWS risorsa in base alla quale si è svolta l'attività che ha portato GuardDuty alla generazione del risultato.
- Scan ID: applicabile ai risultati quando GuardDuty Malware Protection è abilitata, si tratta di un identificatore della scansione antimalware eseguita sui volumi EBS collegati al carico di lavoro dell'istanza EC2 o del container potenzialmente compromessi. Per ulteriori informazioni, consulta Dettagli degli esiti della protezione da malware.
- Gravità: a un esito viene assegnato un livello di gravità, che può essere alto, medio o basso. Per ulteriori informazioni, consulta Livelli di gravità dei GuardDuty risultati.

- Aggiornato il: l'ultima volta che questo risultato è stato aggiornato con una nuova attività che corrisponde allo schema che ha portato GuardDuty alla generazione di questo risultato.

Risorsa

La risorsa interessata fornisce dettagli sulla AWS risorsa presa di mira dall'attività iniziale. Le informazioni disponibili variano in base al tipo di risorsa e al tipo di operazione.

Ruolo della risorsa: il ruolo della AWS risorsa che ha avviato la ricerca. Questo valore può essere TARGET o ACTOR e indica se la risorsa era la destinazione dell'attività sospetta o l'attore che l'ha messa in atto.

Tipo di risorsa: il tipo di risorsa interessata. Un esito può includere diversi tipi di risorse se sono state coinvolte più risorse. I tipi di risorse sono Instance, S3Bucket AccessKey, ECSCluster, Container KubernetesCluster, RDSDBInstance e Lambda. A seconda del tipo di risorsa sono disponibili diversi dettagli degli esiti. Seleziona una scheda delle opzioni di risorsa per scoprire i dettagli disponibili per la risorsa interessata.

Instance

Dettagli dell'istanza:

> **Note**
>
> Potrebbero mancare alcuni dettagli se l'istanza è già stata interrotta o se l'invocazione dell'API sottostante ha avuto origine da un'istanza EC2 in una regione durante una chiamata API tra regioni.

- ID istanza: l'ID dell'istanza EC2 coinvolta nell'attività che ha portato alla generazione del risultato. GuardDuty
- Tipo di istanza: il tipo dell'istanza EC2 coinvolta nell'esito.
- Ora di avvio: la data e l'ora in cui l'istanza è stata avviata.
- Outpost ARN — L'Amazon Resource Name (ARN) di. AWS Outposts Applicabile solo alle istanze. AWS Outposts Per ulteriori informazioni, consulta What is AWS Outposts?
- Nome del gruppo di sicurezza: il nome del gruppo di sicurezza collegato all'istanza interessata.
- ID gruppo di sicurezza: l'ID del gruppo di sicurezza collegato all'istanza interessata.

- Stato dell'istanza: lo stato attuale dell'istanza di destinazione.
- Zona di disponibilità: la zona di disponibilità della regione AWS in cui si trova l'istanza coinvolta.
- ID immagine: l'ID dell'Amazon Machine Image utilizzato per creare l'istanza coinvolta nell'attività.
- Descrizione immagine: una descrizione dell'ID dell'Amazon Machine Image utilizzato per creare l'istanza coinvolta nell'attività.
- Tag: un elenco di tag collegati a questa risorsa elencati nel formato `key:value`.

AccessKey

Dettagli chiave di accesso:

- ID chiave di accesso: l'ID della chiave di accesso dell'utente impegnato nell'attività che ha richiesto GuardDuty la generazione del risultato.
- ID principale: l'ID principale dell'utente impegnato nell'attività che ha richiesto GuardDuty la generazione del risultato.
- Tipo di utente: il tipo di utente impegnato nell'attività che ha richiesto GuardDuty la generazione del risultato. Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail .
- Nome utente: il nome dell'utente impegnato nell'attività che ha richiesto GuardDuty la generazione del risultato.

S3Bucket

Dettagli bucket Amazon S3:

- Nome: il nome del bucket coinvolto nell'esito.
- ARN: l'ARN del bucket coinvolto nell'esito.
- Proprietario: l'ID utente canonico dell'utente proprietario del bucket coinvolto nell'esito. Per ulteriori informazioni sull'ID utente canonico, consulta Identificatori account AWS.
- Tipo: il tipo di esito del bucket può essere Destinazione o Origine.
- Crittografia lato server predefinita: i dettagli di crittografia per il bucket.
- Tag bucket: un elenco dei tag collegati a questa risorsa, elencati nel formato di `key:value`.
- Autorizzazioni valide: una valutazione di tutte le autorizzazioni e le policy valide nel bucket che indica se il bucket interessato è esposto pubblicamente. I valori possono essere Pubblico o Non pubblico.

EKSCluster

Dettagli del cluster Kubernetes:

- Nome: il nome del cluster Kubernetes.
- ARN: l'ARN che identifica il cluster.
- Ora creazione: la data e l'ora di creazione di questo cluster.

> **Note**
>
> I timestamp per i risultati nella GuardDuty console vengono visualizzati nel fuso orario locale, mentre le esportazioni JSON e gli output CLI visualizzano i timestamp in UTC.

- ID VPC: l'ID del VPC associato al cluster.
- Stato: lo stato attuale del cluster.
- Tag: i metadati applicati al cluster utili per catalogarli e organizzarli. Ciascun tag è formato da una chiave e da un valore facoltativo, elencati nel formato `key:value`. Puoi definire sia la chiave che il valore.

  I tag del cluster non si propagano ad altre risorse associate al cluster.

Dettagli del carico di lavoro Kubernetes:

- Tipo: il tipo di carico di lavoro Kubernetes, ad esempio pod, implementazione e processo.
- Nome: il nome del carico di lavoro Kubernetes.
- Uid: l'ID univoco del carico di lavoro Kubernetes.
- Ora creazione: la data e l'ora di creazione di questo carico di lavoro.
- Etichette: le coppie chiave-valore collegate al carico di lavoro Kubernetes.
- Container: i dettagli del container in esecuzione come parte del carico di lavoro Kubernetes.
- Spazio dei nomi: il carico di lavoro appartiene a questo spazio dei nomi Kubernetes.
- Volumi: i volumi utilizzati dal carico di lavoro Kubernetes.
  - Percorso host: rappresenta un file o una directory preesistente sulla macchina host a cui è mappato il volume.
  - Nome: il nome del volume.

- Contesto di sicurezza del pod: definisce i privilegi e le impostazioni di controllo degli accessi per tutti i container in un pod.
- Rete host: impostata su `true` se i pod sono inclusi nel carico di lavoro Kubernetes.

Dettagli utente Kubernetes:

- Gruppi: gruppi Kubernetes RBAC (controllo degli accessi basato sul ruolo) dell'utente coinvolto nell'attività che ha generato l'esito.
- ID: l'ID univoco dell'utente Kubernetes.
- Nome utente: nome dell'utente Kubernetes coinvolto nell'attività che ha generato l'esito.
- Nome sessione: entità che ha assunto il ruolo IAM con le autorizzazioni RBAC di Kubernetes.

ECSCluster

Dettagli del cluster ECS:

- ARN: l'ARN che identifica il cluster.
- Nome: il nome del cluster.
- Stato: lo stato attuale del cluster.
- Numero di servizi attivi: il numero dei servizi in esecuzione sul cluster con stato `ACTIVE`. Puoi visualizzare questi servizi con ListServices
- Numero di istanze di container registrate: il numero delle istanze di container registrate nel cluster, incluse sia le istanza di container con stato `ACTIVE` che quelle con stato `DRAINING`.
- Numero di attività in esecuzione: il numero di attività con stato `RUNNING` nel cluster.
- Tag: i metadati applicati al cluster utili per catalogarli e organizzarli. Ciascun tag è formato da una chiave e da un valore facoltativo, elencati nel formato `key:value`. Puoi definire sia la chiave che il valore.
- Container: i dettagli sul container associato all'attività.
  - Nome container: il nome del container.
  - Immagine del container: l'immagine del container.
- Dettagli dell'attività: i dettagli di un'attività in un cluster.
  - ARN: il nome della risorsa Amazon (ARN) dell'attività.
  - ARN di definizione: il nome della risorsa Amazon (ARN) della definizione dell'attività che crea l'attività.

- Versione: il contatore delle versioni per l'attività.
- Ora creazione attività: il timestamp Unix al momento della creazione dell'attività.
- Ora inizio attività: il timestamp Unix all'inizio dell'attività.
- Attività iniziata da: il tag specificato all'avvio di un'attività.

Container

Dettagli container:

- Runtime del container: il runtime del container (ad esempio `docker` o `containerd`) utilizzato per eseguire il container.
- ID: l'ID dell'istanza di container o le voci ARN complete per l'istanza di container.
- Nome: il nome del container.

  Se disponibile, questo campo mostra il valore dell'etichetta `io.kubenetes.container.name`.
- Immagine: l'immagine dell'istanza di container.
- Montaggi volume: elenco dei montaggi del volume del container. Un container può montare un volume nel proprio file system.
- Contesto di sicurezza: il contesto di sicurezza del container definisce i privilegi e le impostazioni di controllo degli accessi per un container.
- Dettagli del processo: descrive i dettagli del processo associato all'esito.

RDSDBInstance

Dettagli RDSDBInstance:

> **Note**
>
> Questa risorsa è disponibile negli esiti della Protezione RDS relativi all'istanza di database.

- ID dell'istanza del database: l'identificatore associato all'istanza di database coinvolta nella GuardDuty ricerca.

- Motore: il nome del motore di database dell'istanza di database coinvolta nell'esito. I valori possibili sono compatibili con Aurora MySQL o Aurora PostgreSQL.
- Versione del motore: la versione del motore di database coinvolta nel GuardDuty risultato.
- ID del cluster di database: l'identificatore del cluster di database che contiene l'ID dell'istanza di database coinvolta nel GuardDuty risultato.
- ARN dell'istanza di database: l'ARN che identifica l'istanza di database coinvolta nel risultato. GuardDuty

Lambda

Dettagli della funzione Lambda

- Nome funzione: il nome della funzione Lambda coinvolta nell'esito.
- Versione della funzione: la versione della funzione Lambda coinvolta nell'esito.
- Descrizione della funzione: una descrizione della funzione Lambda coinvolta nell'esito.
- Funzione ARN: il nome della risorsa Amazon (ARN) della funzione Lambda coinvolta nell'esito.
- ID revisione: l'ID di revisione della versione della funzione Lambda.
- Ruolo: il ruolo di esecuzione della funzione Lambda coinvolta nell'esito.
- Configurazione VPC: la configurazione di Amazon VPC, inclusi l'ID VPC, il gruppo di sicurezza e gli ID di sottorete associati alla funzione Lambda.
- ID VPC: l'ID dell'Amazon VPC associato alla funzione Lambda coinvolta nell'esito.
- ID sottorete: l'ID delle sottoreti associate alla funzione Lambda.
- Gruppo di sicurezza: il gruppo di sicurezza collegato alla funzione Lambda coinvolta. Sono inclusi il nome e l'ID del gruppo di sicurezza.
- Tag: un elenco di tag collegati a questa risorsa, elencati nel formato della coppia `key:value`.

Dettagli utente del database (DB) RDS

> **Note**
>
> Questa sezione è applicabile ai risultati quando si abilita la funzionalità di protezione RDS in. GuardDuty Per ulteriori informazioni, consulta GuardDuty Protezione RDS.

Il GuardDuty risultato fornisce i seguenti dettagli relativi all'utente e all'autenticazione del database potenzialmente compromesso.

- Utente: il nome utente utilizzato per effettuare il tentativo di accesso anomalo.
- Applicazione: il nome dell'applicazione utilizzata per effettuare il tentativo di accesso anomalo.
- Database: il nome dell'istanza di database coinvolta nel tentativo di accesso anomalo.
- SSL: la versione del Secure Socket Layer (SSL) utilizzata per la rete.
- Metodo di autenticazione: il metodo di autenticazione utilizzato dall'utente coinvolto nell'esito.

Dettagli relativi ai risultati di Runtime Mon

> **Note**
>
> Questi dettagli possono essere disponibili solo se GuardDuty genera uno deiTipi di risultati del monitoraggio del runtime.

Questa sezione contiene i dettagli del runtime, inclusi i dettagli del processo e qualsiasi contesto richiesto. I dettagli del processo descrivono le informazioni sul processo osservato e il contesto di runtime descrive qualsiasi informazione aggiuntiva sull'attività potenzialmente sospetta.

Dettagli del processo

- Nome: il nome del processo.
- Percorso eseguibile: il percorso assoluto del file eseguibile del processo.
- SHA-256 eseguibile: l'hash SHA256 dell'eseguibile del processo.
- PID dello spazio dei nomi: l'ID processo in un PID dello spazio dei nomi secondario diverso dal PID dello spazio dei nomi a livello di host. Per i processi all'interno di un container, corrisponde all'ID processo osservabile nel container.
- Directory di lavoro presente: la directory di lavoro presente del processo.
- ID processo: l'ID che il sistema operativo assegna al processo.
- startTime: l'ora in cui è iniziato il processo. Si presenta nel formato della stringa di data UTC (`2023-03-22T19:37:20.168Z`).
- UUID: l'ID univoco assegnato al processo da. GuardDuty

- UUID padre: l'ID univoco del processo padre. Questo ID viene assegnato al processo principale da. GuardDuty
- Utente: l'utente che ha eseguito il processo.
- ID utente: l'ID dell'utente che ha eseguito il processo.
- ID utente effettivo: l'ID utente effettivo del processo al momento dell'evento.
- Eredità: informazioni sugli antenati del processo.
  - ID processo: l'ID che il sistema operativo assegna al processo.
  - UUID: l'ID univoco assegnato al processo da. GuardDuty
  - Percorso eseguibile: il percorso assoluto del file eseguibile del processo.
  - ID utente effettivo: l'ID utente effettivo del processo al momento dell'evento.
  - UUID padre: l'ID univoco del processo padre. Questo ID viene assegnato al processo principale da. GuardDuty
  - Ora di inizio: l'ora in cui è iniziato il processo.
  - PID dello spazio dei nomi: l'ID processo in un PID dello spazio dei nomi secondario diverso dal PID dello spazio dei nomi a livello di host. Per i processi all'interno di un container, corrisponde all'ID processo osservabile nel container.
  - ID utente: l'ID utente dell'utente che ha eseguito il processo.
  - Nome: il nome del processo.

Contesto di runtime

Un esito generato può includere, tra i campi seguenti, solo quelli pertinenti al tipo di esito.

- Origine di montaggio: il percorso sull'host montato dal container.
- Destinazione di montaggio: il percorso nel container mappato alla directory host.
- Tipo di file system: rappresenta il tipo di file system montato.
- Flag: rappresenta le opzioni che controllano il comportamento dell'evento coinvolto in questo esito.
- Processo di modifica: informazioni sul processo che in fase di runtime ha creato o modificato un file binario, uno script o una libreria all'interno di un container.
- Ora della modifica: il timestamp in cui il processo ha creato o modificato un file binario, uno script o una libreria all'interno di un container in fase di runtime. Questo campo è nel formato della stringa di data UTC (`2023-03-22T19:37:20.168Z`).
- Percorso libreria: il percorso della nuova libreria che è stata caricata.

- Valore LD Preload: il valore della variabile di ambiente `LD_PRELOAD`.
- Percorso socket: il percorso del socket Docker a cui è stato effettuato l'accesso.
- Percorso binario runc: il percorso del file binario `runc`.
- Percorso agente di rilascio: il percorso del file dell'agente di rilascio `cgroup`.
- Esempio di riga di comando: l'esempio della riga di comando coinvolta nell'attività potenzialmente sospetta.
- Categoria utensile: categoria a cui appartiene lo strumento. Alcuni esempi sono Backdoor Tool, Pentest Tool, Network Scanner e Network Sniffer.
- Nome dello strumento: il nome dello strumento potenzialmente sospetto.
- Percorso dello script: il percorso dello script eseguito che ha generato il risultato.
- Threat File Path: il percorso sospetto per il quale sono stati trovati i dettagli di intelligence sulle minacce.
- Nome del servizio: il nome del servizio di sicurezza che è stato disabilitato.

Dettagli della scansione dei volumi EBS

> **Note**
>
> Questa sezione è applicabile ai risultati ottenuti quando si attiva la scansione antimalware GuardDuty avviata. GuardDuty Protezione da malware

La scansione dei volumi EBS fornisce dettagli sul volume EBS collegato all'istanza EC2 o al carico di lavoro di un container potenzialmente compromessi.

- ID scansione: l'identificatore della scansione malware.
- Ora inizio scansione: la data e l'ora di inizio della scansione malware.
- Ora completamento scansione: la data e l'ora di completamento della scansione malware.
- Trigger Finding ID: l'ID di ricerca del GuardDuty risultato che ha avviato questa scansione antimalware.
- Origini: i valori possibili sono `Bitdefender` e `AWS`.
- Rilevamenti scansione: la visualizzazione completa dei dettagli e degli esiti di ogni scansione malware.

- Numero elementi scansionati: il numero totale di file scansionati. Fornisce dettagli come `totalGb`, `files` e `volumes`.
- Numero elementi rilevati come minacce: il numero totale di `files` dannosi rilevati durante la scansione.
- Dettagli sulla minaccia con gravità più alta: i dettagli sulla minaccia di gravità più alta rilevata durante la scansione e sul numero di file dannosi. Fornisce dettagli come `severity`, `threatName` e `count`.
- Minacce rilevate per nome: l'elemento container che raggruppa le minacce di tutti i livelli di gravità. Fornisce dettagli come `itemCount`, `uniqueThreatNameCount`, `shortened` e `threatNames`.

Dettagli degli esiti della protezione da malware

> **Note**
>
> Questa sezione è applicabile ai risultati ottenuti quando si attiva la scansione GuardDuty antimalware avviata. GuardDuty Protezione da malware

Quando la scansione della protezione da malware rileva un malware, puoi visualizzare i dettagli della scansione selezionando l'esito corrispondente nella pagina Risultati della console https://console.aws.amazon.com/guardduty/ La gravità del rilevamento relativo alla protezione da malware dipende dalla gravità del GuardDuty rilevamento.

> **Note**
>
> Il tag `GuardDutyFindingDetected` specifica che gli snapshot contengono malware.

Le seguenti informazioni sono disponibili nella sezione Minacce rilevate nel pannello dei dettagli.

- Nome: il nome della minaccia, ottenuto raggruppando i file in base al rilevamento.
- Gravità: la gravità della minaccia rilevata.
- Hash: l'hash SHA-256 del file.
- Percorso file: la posizione del file dannoso nel volume EBS.
- Nome file: il nome del file in cui è stata rilevata la minaccia.

- ARN del volume: l'ARN dei volumi EBS scansionati.

Le seguenti informazioni sono disponibili nella sezione Dettagli della scansione malware nel pannello dei dettagli.

- ID scansione: l'ID di scansione della scansione malware.
- Ora inizio scansione: la data e l'ora di inizio della scansione.
- Ora completamento scansione: la data e l'ora di completamento della scansione.
- File scansionati: il numero totale di file e directory scansionati.
- GB totali scansionati: la quantità di spazio di archiviazione scansionato durante il processo.
- Trigger Finding ID: l'ID identificativo del GuardDuty risultato che ha avviato questa scansione antimalware.
- Le seguenti informazioni sono disponibili nella sezione Dettagli del volume nel pannello dei dettagli.
  - ARN del volume: il nome della risorsa Amazon (ARN) del volume.
  - SnapshotARN: l'ARN dello snapshot del volume EBS.
  - Stato: lo stato della scansione del volume, ad esempio, `Running`, `Skipped` e `Completed`.
  - Tipo di crittografia: il tipo di crittografia utilizzato per crittografare il volume. Ad esempio, `CMCMK`.
  - Nome dispositivo: il nome del dispositivo. Ad esempio, `/dev/xvda`.

Azione

L'Operazione di un esito fornisce dettagli sul tipo di attività che l'ha attivato. Le informazioni disponibili variano in base al tipo di operazione.

Tipo di operazione: il tipo di attività dell'esito. Questo valore può essere NETWORK_CONNECTION, PORT_PROBE, DNS_REQUEST, AWS_API_CALL o RDS_LOGIN_ATTEMPT. Le informazioni disponibili variano in base al tipo di operazione:

- NETWORK_CONNECTION: indica che il traffico di rete è stato scambiato tra l'istanza EC2 identificata e l'host remoto. Questo tipo di operazione include le seguenti informazioni aggiuntive:
  - Direzione della connessione: la direzione della connessione di rete osservata nell'attività che ha richiesto GuardDuty la generazione del risultato. Può essere uno dei seguenti valori:
    - INBOUND: indica che un host remoto ha avviato una connessione a una porta locale sull'istanza EC2 identificata nel tuo account.

    - OUTBOUND: indica che l'istanza EC2 identificata ha avviato una connessione a un host remoto.
    - SCONOSCIUTA: indica che non è GuardDuty stato possibile determinare la direzione della connessione.
  - Protocollo: il protocollo di connessione di rete osservato nell'attività che ha richiesto GuardDuty la generazione del risultato.
  - IP locale: il primo indirizzo IP di origine del traffico che ha attivato l'esito. Queste informazioni possono essere utilizzate per distinguere tra indirizzo IP di un livello intermedio su cui fluisce il traffico e il primo indirizzo IP di origine del traffico. Ad esempio, l'indirizzo IP di un pod EKS anziché l'indirizzo IP dell'istanza in cui è in esecuzione il pod EKS.
  - Bloccata: indica se la porta di destinazione è bloccata.
- PORT_PROBE: indica che 'istanza EC2 identificata è stata sottoposta a probing da un host remoto su più porte aperte. Questo tipo di operazione include le seguenti informazioni aggiuntive:
  - IP locale: il primo indirizzo IP di origine del traffico che ha attivato l'esito. Queste informazioni possono essere utilizzate per distinguere tra indirizzo IP di un livello intermedio su cui fluisce il traffico e il primo indirizzo IP di origine del traffico. Ad esempio, l'indirizzo IP di un pod EKS anziché l'indirizzo IP dell'istanza in cui è in esecuzione il pod EKS.
  - Bloccata: indica se la porta di destinazione è bloccata.
- DNS_REQUEST: indica che l'istanza EC2 identificata ha eseguito query in un nome di dominio. Questo tipo di operazione include le seguenti informazioni aggiuntive:
  - Protocollo: il protocollo di connessione di rete osservato nell'attività che ha portato GuardDuty alla generazione del risultato.
  - Bloccata: indica se la porta di destinazione è bloccata.
- AWS_API_CALL: indica che è stata richiamata un'API AWS . Questo tipo di operazione include le seguenti informazioni aggiuntive:
  - API: il nome dell'operazione API che è stata richiamata e quindi richiesta di GuardDuty generare questo risultato.

    > **Note**
    >
    > Queste operazioni possono anche includere eventi non API acquisiti da AWS CloudTrail. Per ulteriori informazioni, consulta Eventi non API acquisiti da. CloudTrail

  - Agente utente: l'agente utente che ha effettuato la richiesta API. Questo valore indica se la chiamata è stata effettuata da AWS Management Console, un AWS servizio, dagli AWS SDK o dal. AWS CLI
  - CODICE DI ERRORE: se l'esito è stato attivato da una chiamata API non riuscita, viene visualizzato il codice di errore per tale chiamata.
  - Nome servizio: il nome DNS del servizio che ha tentato di effettuare la chiamata API che ha attivato l'esito.
- RDS_LOGIN_ATTEMPT: indica che è stato effettuato un tentativo di accesso al database potenzialmente compromesso da un indirizzo IP remoto.
  - Indirizzo IP: l'indirizzo IP remoto utilizzato per effettuare il tentativo di accesso potenzialmente sospetto.

Attore o destinazione

Un esito ha una sezione Attore se il Ruolo risorsa era `TARGET`. Ciò indica che la risorsa è stata la destinazione di attività sospette e la sezione Attore contiene dettagli sull'entità che ha scelto come destinazione la risorsa.

Un esito ha una sezione Destinazione se il Ruolo risorsa era `ACTOR`. Ciò indica che la risorsa è stata coinvolta in attività sospette nei confronti di un host remoto e questa sezione contiene informazioni sull'IP o sul dominio di destinazione della risorsa.

Le informazioni disponibili nella sezione Attore o Destinazione possono includere quanto segue:

- Affiliato: indica se l' AWS account del chiamante API remoto è correlato al tuo ambiente. GuardDuty Se questo valore è `true`, il chiamante API è affiliato in qualche modo al tuo account. Se invece il valore è `false`, il chiamante API proviene da un ambiente esterno.
- ID account remoto: l'ID dell'account che possiede l'indirizzo IP in uscita utilizzato per accedere alla risorsa sulla rete finale.
- Indirizzo IP: l'indirizzo IP coinvolto nell'attività che ha richiesto GuardDuty la generazione del risultato.
- Posizione: informazioni sulla posizione dell'indirizzo IP coinvolto nell'attività che ha portato GuardDuty alla generazione del risultato.
- Organizzazione: informazioni sull'organizzazione dell'ISP relative all'indirizzo IP coinvolto nell'attività che ha portato GuardDuty alla generazione del risultato.

- Porta: il numero di porta coinvolto nell'attività che ha portato GuardDuty alla generazione del risultato.
- Dominio: il dominio coinvolto nell'attività che ha portato GuardDuty alla generazione del risultato.
- Dominio con suffisso: il dominio di secondo e primo livello coinvolto in un'attività che potenzialmente ha richiesto GuardDuty la generazione del risultato. Per un elenco dei domini di primo e secondo livello, consulta l'elenco dei suffissi pubblici.

Informazioni aggiuntive

Tutti gli esiti hanno una sezione Informazioni aggiuntive che può includere le informazioni seguenti:

- Nome dell'elenco delle minacce: il nome dell'elenco delle minacce che include l'indirizzo IP o il nome di dominio coinvolto nell'attività che ha richiesto GuardDuty la generazione del risultato.
- Esempio: un valore vero o falso che indica se si tratta di un esito di esempio.
- Archiviato: un valore vero o falso che indica se l'esito è stato archiviato.
- Insolito: dettagli dell'attività che non sono stati osservati in precedenza. Questi dettagli possono includere utente, posizione, bucket, comportamento di accesso od Org ASN anomali (non osservati in precedenza).
- Protocollo insolito: il protocollo di connessione di rete coinvolto nell'attività che ha portato GuardDuty alla generazione del risultato.
- Dettagli dell'agente: dettagli sull'agente di sicurezza attualmente implementato nel cluster EKS del tuo Account AWS. Questi dettagli sono applicabili solo ai tipi di esiti del monitoraggio del runtime EKS.
  - Versione dell'agente: la versione del GuardDuty security agent.
  - ID agente: l'identificatore univoco del GuardDuty security agent.

Evidenza

Gli esiti basati sull'intelligence sulle minacce hanno una sezione Evidenza che include le informazioni seguenti:

- Dettagli di intelligence sulle minacce: il nome dell'elenco delle minacce in cui `Threat name` compaiono le minacce riconosciute.
- Nome della minaccia: il nome della famiglia di malware o altro identificatore associato alla minaccia.

- File di minaccia SHA256: SHA256 del file che ha generato la scoperta.

Comportamento anomalo

I tipi di risultati che terminano con AnomalousBehaviorindicano che il risultato è stato generato dal modello di apprendimento automatico per il rilevamento delle GuardDuty anomalie (ML). Il modello di ML valuta tutte le richieste API al tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta.

I dettagli su quali fattori della richiesta API sono insoliti per l'identità CloudTrail dell'utente che ha richiamato la richiesta sono disponibili nei dettagli del risultato. Le identità sono definite dall'elemento CloudTrail userIdentity e i valori possibili sono`Root`:`IAMUser`,,, `AssumedRole` `FederatedUser`AWSAccount, o. `AWSService`

Oltre ai dettagli disponibili per tutti i GuardDuty risultati associati all'attività dell'API, AnomalousBehaviori risultati contengono dettagli aggiuntivi descritti nella sezione seguente. Questi dettagli possono essere visualizzati nella console e sono disponibili anche nel JSON dell'esito.

- API anomale: un elenco di richieste API richiamate dall'identità utente in prossimità della richiesta API principale associata all'esito. Questo riquadro suddivide ulteriormente i dettagli dell'evento API nei modi seguenti.
  - La prima API elencata è l'API principale, ossia la richiesta API associata all'attività osservata con il rischio più elevato. Si tratta dell'API che ha attivato l'esito ed è correlata alla fase di attacco del tipo di esito. L'API in questione è descritta in dettaglio nella sezione Operazione della console e nel JSON dell'esito.
  - Tutte le altre API elencate sono API anomale aggiuntive dell'identità utente riportata che è stata osservata in prossimità dell'API principale. Se nell'elenco è presente una sola API, il modello di ML non ha identificato come anomala alcuna richiesta API aggiuntiva proveniente dall'identità utente.
  - L'elenco delle API viene suddiviso in base al fatto che un'API sia stata chiamata correttamente o che sia stata chiamata senza successo, il che significa che è stata ricevuta una risposta di errore. Il tipo di risposta di errore ricevuta è elencato sopra ogni API chiamata senza successo. I possibili tipi di risposta di errore sono: `access denied`, `access denied exception`, `auth failure`, `instance limit exceeded`, `invalid permission - duplicate`, `invalid permission - not found` e `operation not permitted`.

- Le API sono classificate in base al servizio associato.

> **Note**
>
> Per maggiori informazioni, scegli API storiche per visualizzare i dettagli sulle API principali, fino a un massimo di 20, che di solito vengono visualizzate sia per l'identità utente che per tutti gli utenti all'interno dell'account. Le API sono contrassegnate come Rare (meno di una volta al mese), Poco frequenti (alcune volte al mese) o Frequenti (da giornaliera a settimanale), a seconda della frequenza con cui vengono utilizzate all'interno dell'account.

- Comportamento insolito (account): questa sezione fornisce ulteriori dettagli sul comportamento profilato del tuo account. Le informazioni registrate in questo pannello includono:
  - Org ASN: l'Org ASN da cui è stata effettuata la chiamata API anomala.
  - Nome utente: il nome dell'utente che ha effettuato la chiamata API anomala.
  - Agente utente: l'agente utente utilizzato per effettuare la chiamata API anomala. L'agente utente è il metodo utilizzato per effettuare la chiamata, ad esempio `aws-cli` o `Botocore`.
  - Tipo utente: il tipo di utente che ha effettuato la chiamata API anomala. I valori possibili sono `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` o `ROLE`.
  - Bucket: il nome del bucket S3 a cui viene effettuato l'accesso.
- Comportamento insolito (identità utente): questa sezione fornisce ulteriori dettagli sul comportamento profilato dell'Identità utente coinvolta nell'esito. Quando un comportamento non è identificato come storico, significa che il modello GuardDuty ML non aveva mai visto l'identità dell'utente effettuare questa chiamata API in questo modo durante il periodo di formazione. Sono disponibili i seguenti dettagli aggiuntivi sull'Identità utente:
  - Org ASN: l'Org ASN da cui è stata effettuata la chiamata API anomala.
  - Agente utente: l'agente utente utilizzato per effettuare la chiamata API anomala. L'agente utente è il metodo utilizzato per effettuare la chiamata, ad esempio `aws-cli` o `Botocore`.
  - Bucket: il nome del bucket S3 a cui viene effettuato l'accesso.
- Comportamento insolito (bucket): questa sezione fornisce ulteriori dettagli sul comportamento profilato del bucket S3 associato all'esito Quando un comportamento non è identificato come storico, significa che il modello GuardDuty ML non aveva mai visto in precedenza chiamate API effettuate a questo bucket in questo modo durante il periodo di formazione. Le informazioni registrate in questa sezione includono:
  - Org ASN: l'Org ASN da cui è stata effettuata la chiamata API anomala.

- Nome utente: il nome dell'utente che ha effettuato la chiamata API anomala.
- Agente utente: l'agente utente utilizzato per effettuare la chiamata API anomala. L'agente utente è il metodo utilizzato per effettuare la chiamata, ad esempio `aws-cli` o `Botocore`.
- Tipo utente: il tipo di utente che ha effettuato la chiamata API anomala. I valori possibili sono `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` o `ROLE`.

> **Note**
>
> Per maggiori informazioni sui comportamenti storici, scegli Comportamento storico nella sezione Comportamento insolito (account), ID utente o Bucket per visualizzare i dettagli sul comportamento previsto nel tuo account per ciascuna delle seguenti categorie: Raro (meno di una volta al mese), Poco frequente (alcune volte al mese) o Frequente (da giornaliero a settimanale), a seconda della frequenza con cui vengono utilizzati all'interno del tuo account.

- Comportamento insolito (database): questa sezione fornisce ulteriori dettagli sul comportamento profilato dell'istanza di database associata all'esito Quando un comportamento non è identificato come storico, significa che il modello GuardDuty ML non ha mai visto in precedenza un tentativo di accesso effettuato in questo modo a questa istanza di database durante il periodo di formazione. Le informazioni registrate nel pannello dell'esito per questa sezione includono:
  - Nome utente: il nome utente utilizzato per effettuare il tentativo di accesso anomalo.
  - Org ASN: l'Org ASN da cui è stato effettuato il tentativo di accesso anomalo.
  - Nome applicazione: il nome dell'applicazione utilizzata per effettuare il tentativo di accesso anomalo.
  - Nome database: il nome dell'istanza di database coinvolta nel tentativo di accesso anomalo.

> **Note**
>
> La sezione Comportamento storico fornisce maggiori informazioni su Nomi utente, Org ASN, Nomi applicazioni e Nomi database osservati in precedenza per il database associato. A ogni valore univoco è associato un conteggio che rappresenta il numero di volte in cui questo valore è stato osservato in un evento di accesso riuscito.

- Comportamento insolito (account cluster Kubernetes, spazio dei nomi Kubernetes e nome utente Kubernetes): questa sezione fornisce ulteriori dettagli sul comportamento profilato per il cluster e lo spazio dei nomi Kubernetes associati all'esito. Quando un comportamento non è identificato

come storico, significa che il modello GuardDuty ML non ha mai osservato in precedenza questo account, cluster, namespace o nome utente in questo modo. Le informazioni registrate nel pannello dell'esito per questa sezione includono:

- Nome utente: l'utente che ha chiamato l'API Kubernetes associata all'esito.
- Nome utente impersonato: l'utente impersonato da `username`.
- Spazio dei nomi: lo spazio dei nomi Kubernetes all'interno del cluster Amazon EKS in cui si è verificata l'operazione.
- Agente utente: l'agente utente associato alla chiamata API Kubernetes. L'agente utente è il metodo utilizzato per effettuare la chiamata, ad esempio `kubectl`.
- API: l'API Kubernetes chiamata da `username` all'interno del cluster Amazon EKS.
- Informazioni ASN: le informazioni ASN, come Organizzazione e ISP, associate all'indirizzo IP dell'utente che effettua questa chiamata.
- Giorno della settimana: il giorno della settimana in cui è stata effettuata la chiamata API Kubernetes.
- Autorizzazione[1]: il verbo e la risorsa Kubernetes di cui viene verificato l'accesso per indicare se `username` può utilizzare o meno l'API Kubernetes.
- Nome dell'account di servizio[1]: l'account di servizio associato al carico di lavoro Kubernetes che fornisce un'identità al carico di lavoro.
- Registro[1]: il registro del container associato all'immagine del container che viene implementata nel carico di lavoro Kubernetes.
- Immagine[1]: l'immagine del container, senza i tag e il digest associati, che viene implementata nel carico di lavoro Kubernetes.
- Configurazione prefisso immagine[1]: il prefisso dell'immagine con la configurazione di sicurezza del container e del carico di lavoro abilitata, ad esempio `hostNetwork` o `privileged`, per il container che utilizza l'immagine.
- Nome soggetto[1]: il soggetto, ad esempio `user`, `group` o `serviceAccountName` che è associato a un ruolo di riferimento in un `RoleBinding` o `ClusterRoleBinding`.
- Nome ruolo[1]: il nome del ruolo coinvolto nella creazione o nella modifica di ruoli o l'API `roleBinding`.

Anomalie basate sul volume S3

Questa sezione descrive in dettaglio le informazioni contestuali per le anomalie basate sul volume S3. L'esito basato sul volume (Exfiltration:S3/AnomalousBehavior) monitora il numero insolito di

chiamate API S3 effettuate dagli utenti ai bucket S3, indicando una potenziale esfiltrazione di dati. Le seguenti chiamate API S3 vengono monitorate per rilevare eventuali anomalie basate sul volume.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

Le metriche seguenti possono essere utili per creare una linea di base del comportamento abituale quando un'entità IAM accede a un bucket S3. Per identificare un'eventuale esfiltrazione di dati, l'esito del rilevamento delle anomalie basato sul volume valuta tutte le attività rispetto alla consueta linea di base comportamentale. Scegli Comportamento storico nelle sezioni Comportamento insolito (identità utente), Volume osservato (identità utente) e Volume osservato (Bucket) per visualizzare rispettivamente le metriche seguenti.

- Numero di chiamate API `s3-api-name` richiamate dall'utente o dal ruolo IAM (in base a quello emesso) associate al bucket S3 interessato nelle ultime 24 ore.
- Numero di chiamate API `s3-api-name` richiamate dall'utente o dal ruolo IAM (in base a quello emesso) associate a tutti i bucket S3 interessati nelle ultime 24 ore.
- Numero di chiamate API `s3-api-name` su tutti gli utenti o ruoli IAM (in base a quelli emesso) associate al bucket S3 interessato nelle ultime 24 ore.

Anomalie basate sull'attività di accesso RDS

Questa sezione descrive in dettaglio il conteggio dei tentativi di accesso eseguiti dall'attore insolito ed è raggruppata in base al risultato dei tentativi di accesso. Tipi di esiti della Protezione RDS identifica comportamenti anomali monitorando gli eventi di accesso alla ricerca di schemi insoliti di `successfulLoginCount`, `failedLoginCount` e `incompleteConnectionCount`.

- successfulLoginCount— Questo contatore rappresenta la somma delle connessioni riuscite (combinazione corretta di attributi di accesso) effettuate all'istanza del database dall'attore insolito. Gli attributi di accesso includono nome utente, password e nome del database.
- failedLoginCount— Questo contatore rappresenta la somma dei tentativi di accesso falliti (non riusciti) effettuati per stabilire una connessione all'istanza del database. Ciò indica che uno o più attributi della combinazione di accesso, ad esempio nome utente, password o nome del database, erano errati.

- incompleteConnectionCount— Questo contatore rappresenta il numero di tentativi di connessione che non possono essere classificati come riusciti o falliti. Queste connessioni vengono chiuse prima che il database fornisca una risposta. Ad esempio, la scansione delle porte viene effettuata dove è connessa la porta del database, ma al database non viene inviata alcuna informazione oppure la connessione è stata interrotta prima del completamento di un tentativo di accesso riuscito o fallito.

Formato degli esiti di GuardDuty

GuardDuty genera un esito se rileva un comportamento sospetto o non previsto nel tuo ambiente AWS. Un esito è una notifica che contiene i dettagli su un potenziale problema di sicurezza rilevato da GuardDuty. I dettagli degli esiti includono informazioni su quanto è accaduto, sulle risorse AWS coinvolte nell'attività sospetta, sul momento in cui questa è avvenuta e molto altro.

Una delle informazioni più utili di questi dettagli è il tipo di risultato. La funzione del tipo di risultato è di fornire una descrizione concisa ma intelligibile del potenziale problema di sicurezza. Ad esempio, il tipo di esito di GuardDuty Recon:EC2/PortProbeUnprotectedPort ti informa rapidamente che una porta non protetta di un'istanza EC2 nel tuo ambiente AWS è sottoposta a probing da parte di un potenziale utente malintenzionato.

GuardDuty utilizza il formato seguente per nominare i vari tipi di esiti che genera:

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName.DetectionMechanism!Artifact

Ogni parte di questo formato rappresenta un aspetto di un tipo di esito. Di seguito le spiegazioni di questi aspetti:

- ThreatPurpose: descrive l'obiettivo principale di una minaccia, di un tipo di attacco o della fase di un potenziale attacco. Consulta la sezione seguente per un elenco completo degli scopi delle minacce GuardDuty.
- ResourceTypeAffected: descrive il tipo di risorse AWS identificate in questo esito come potenziali destinazioni di un attacco. Attualmente, GuardDuty è in grado di generare esiti per le risorse EC2, S3, IAM ed EKS.
- ThreatFamilyName: descrive la minaccia o la potenziale attività dannosa globale in corso di rilevamento da parte di GuardDuty. Ad esempio, il valore NetworkPortUnusual indica che un'istanza EC2 identificata nell'esito di GuardDuty non ha mai comunicato su una determinata porta remota (anch'essa identificata nell'esito) in precedenza.

- DetectionMechanism: descrive il metodo con cui GuardDuty ha rilevato l'esito. Questo aspetto può essere utilizzato per indicare la variazione di un tipo di esito comune o un esito che GuardDuty ha rilevato utilizzando un meccanismo specifico. Ad esempio, Backdoor:EC2/DenialOfService.Tcp indica che il Denial of Service (DoS) è stato rilevato tramite TCP. La variante UDP è Backdoor:EC2/DenialOfService.Udp.

  Il valore .Custom indica che GuardDuty ha rilevato l'esito in base agli elenchi minacce personalizzati, mentre .Reputation indica che GuardDuty ha rilevato l'esito utilizzando un modello di punteggio di reputazione del dominio.
- Artefatto: descrive una risorsa specifica di proprietà di uno strumento utilizzato nell'attività dannosa. Ad esempio, DNS nel tipo di risultato CryptoCurrency:EC2/BitcoinTool.B!DNS indica che un'istanza EC2 sta comunicando con un noto dominio correlato al bitcoin.

Scopi delle minacce

In GuardDuty, lo scopo della minaccia descrive l'obiettivo principale di una minaccia, di un tipo di attacco o della fase di un potenziale attacco. Ad esempio, alcuni scopi delle minacce, come Backdoor, indicano un tipo di attacco. Tuttavia, alcuni scopi delle minacce, come Impatto, sono in linea con le Tattiche MITRE ATT&CK. Le tattiche MITRE ATT&CK indicano diverse fasi del ciclo di attacco di un avversario. Nella versione corrente di GuardDuty, ThreatPurpose può avere i valori seguenti:

Backdoor

Questo valore indica che un avversario ha compromesso una risorsa AWS e l'ha alterata in modo da riuscire a contattare il relativo server di comando e controllo (C&C) per ricevere ulteriori istruzioni a fini dannosi.

Comportamento

Questo valore indica che GuardDuty ha rilevato un'attività o modelli di attività che differiscono dalla linea di base stabilita per la risorsa AWS coinvolta.

CredentialAccess

Questo valore indica che GuardDuty ha rilevato modelli di attività che un avversario potrebbe utilizzare per rubare credenziali, come ID account o password, dal tuo ambiente. Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK

Criptovalute

Questo valore indica che GuardDuty ha rilevato che una risorsa AWS nel tuo ambiente ospita un software associato a criptovalute (ad esempio, Bitcoin).

DefenseEvasion

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che un avversario potrebbe utilizzare per non essere rilevato mentre si infiltra nel tuo ambiente. Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK

Individuazione

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che un avversario potrebbe utilizzare per ampliare la propria conoscenza dei sistemi e delle reti interne. Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK.

Esecuzione

Questo valore indica che GuardDuty ha rilevato che un avversario potrebbe tentare di eseguire codice dannoso per esplorare la rete o rubare dati. Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK .

Esfiltrazione

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che un avversario potrebbe utilizzare per tentare di rubare dati dalla rete. Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK.

Impatto

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che suggeriscono il tentativo di un avversario di manipolare, interrompere o distruggere i sistemi e i dati. Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK

InitialAccess

Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK

Test di penetrazione (pen-test)

A volte i proprietari di risorse AWS o i loro rappresentanti autorizzati eseguono intenzionalmente dei test su determinate applicazioni AWS per identificarne le vulnerabilità, come gruppi di sicurezza aperti o chiavi di accesso troppo permissive. Questi test di penetrazione vengono

eseguiti nel tentativo di identificare e bloccare le risorse vulnerabili prima che siano individuate dagli avversari. Tuttavia, alcuni degli strumenti utilizzati dai tester autorizzati sono disponibili gratuitamente e quindi possono essere utilizzati da utenti non autorizzati o malintenzionati per eseguire test di probing. Sebbene GuardDuty non sia in grado di identificare il vero scopo di tale attività, il valore Test di penetrazione (pen-test) indica che GuardDuty rileva un'attività simile a quella generata da strumenti di test di penetrazione noti, attività che potrebbe indicare un'azione di probing dannosa della rete.

Persistence

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che un avversario potrebbe utilizzare per cercare di mantenere l'accesso ai sistemi anche se la loro via di accesso iniziale è interrotta. Ad esempio, ciò potrebbe includere la creazione di un nuovo utente IAM dopo aver ottenuto l'accesso tramite le credenziali compromesse di un utente esistente. Quando le credenziali dell'utente esistente vengono eliminate, l'avversario manterrà l'accesso al nuovo utente che non è stato rilevato come parte dell'evento originale. Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK.

Policy

Questo valore indica che il tuo account Account AWS ha un comportamento che va contro le best practice di sicurezza consigliate.

PrivilegeEscalation

Questo valore indica che il principale coinvolto nel tuo ambiente AWS ha un comportamento che un avversario potrebbe utilizzare per ottenere autorizzazioni di livello superiore per accedere alla rete. Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK.

Recon

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che un avversario potrebbe utilizzare per eseguire la ricognizione della rete in modo da capire come ampliare il proprio accesso o utilizzare le tue risorse. Ad esempio, questa attività può includere l'individuazione delle vulnerabilità presenti nel tuo ambiente AWS controllando le porte, elencando gli utenti e le tabelle del database e così via.

Stealth

Questo valore indica che un avversario cerca attivamente di nascondere le proprie operazioni. Ad esempio, potrebbe utilizzare un server proxy anonimo, il che rende estremamente difficile valutare la vera natura dell'attività.

Trojan

Questo valore indica che un attacco utilizza programmi Trojan per svolgere attività dannose di nascosto. A volte questo software assume l'aspetto di un programma legittimo che gli utenti eseguono quindi involontariamente. In altre, questo software si esegue automaticamente sfruttando una vulnerabilità.

UnauthorizedAccess

Questo valore indica che GuardDuty rileva un'attività o un modello di attività sospetto da parte di un individuo non autorizzato.

Generazione di risultati campionari in GuardDuty

Puoi generare risultati di esempio con Amazon GuardDuty per aiutarti a visualizzare e comprendere i vari tipi di risultati che GuardDuty possono generare. Quando generi risultati di esempio, GuardDuty compila l'elenco dei risultati attuali con un risultato di esempio per ogni tipo di risultato supportato.

Gli esempi generati sono approssimazioni compilate con valori segnaposto. Questi esempi possono apparire diversi dai risultati reali relativi all'ambiente in uso, ma è possibile utilizzarli per testare diverse configurazioni GuardDuty, ad esempio CloudWatch eventi o filtri. Nella tabella Tipi di esiti è riportato un elenco dei valori disponibili per i tipi di esiti.

Per generare alcuni risultati comuni basati su attività simulate all'interno dell'ambiente, vedere Generazione automatica di GuardDuty risultati comuni di seguito.

Generazione di risultati di esempio tramite la GuardDuty console o l'API

Scegli il metodo di accesso che preferisci per generare esiti di esempio.

> **Note**
>
> Utilizzando la console puoi generare un esito per ogni tipo, mentre singoli esiti di esempio possono essere generati solo tramite l'API.

Console

Utilizza la procedura seguente per generare esiti di esempio. Questo processo genera un risultato di esempio per ogni tipo di GuardDuty risultato.

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella pagina Settings (Impostazioni), in Sample findings (Risultati di esempio), selezionare Generate sample findings (Genera risultati di esempio).
4. Nel riquadro di navigazione, seleziona Esiti. Gli esiti di esempio vengono visualizzati nella pagina Risultati attuali con il prefisso [ESEMPIO].

API/CLI

È possibile generare un singolo risultato di esempio corrispondente a qualsiasi tipo di GuardDuty risultato tramite l'CreateSampleFindingsAPI, i valori disponibili per la ricerca dei tipi sono elencati nella Tipi di esiti tabella.

Ciò è utile per testare le regole o l'automazione degli CloudWatch eventi in base ai risultati. L'esempio seguente mostra come generare un singolo esempio di esito del tipo `Backdoor:EC2/DenialOfService.Tcp` utilizzando la AWS CLI.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --finding-types Backdoor:EC2/DenialOfService.Tcp
```

Il titolo degli esiti di esempio generati con questi metodi inizia sempre con [ESEMPIO] nella console. Gli esiti di esempio hanno un valore di `"sample": true` nella sezione AdditionalInfo dei dettagli JSON degli esiti.

Generazione automatica di GuardDuty risultati comuni

È possibile utilizzare i seguenti script per generare automaticamente diversi GuardDuty risultati comuni. Il guardduty-tester.template utilizza AWS CloudFormation per creare un ambiente isolato con un bastion host, un'istanza Amazon EC2 tester a cui puoi accedere tramite SSH e due istanze EC2 di destinazione. Quindi puoi eseguire guardduty_tester.sh per avviare un'interazione tra l'istanza EC2 tester, l'istanza Windows EC2 di destinazione e l'istanza Linux EC2 di destinazione, per simulare cinque tipi di attacchi comuni in grado di rilevare e notificare i risultati generati. GuardDuty

1. Come prerequisito, è necessario abilitarlo nell'account e nella regione GuardDuty in cui si desidera eseguire guardduty-tester.template e guardduty_tester.sh. Per ulteriori informazioni sull'attivazione, vedere. GuardDuty Guida introduttiva con GuardDuty

   Devi generare anche una nuova coppia di chiavi EC2, o utilizzarne una esistente, in ciascuna regione in cui desideri eseguire questi script. Questa coppia di chiavi EC2 viene utilizzata come parametro nello script guardduty-tester.template che usi per creare un nuovo stack. CloudFormation Per ulteriori informazioni sulla generazione delle coppie di chiavi, consulta Coppie di chiavi Amazon EC2.

2. Crea un nuovo stack usando guardduty-tester.template. CloudFormation Per istruzioni dettagliate sulla creazione di uno stack, consulta Creazione di uno stack. Prima di eseguire guardduty-tester.template, modificarlo con i valori per i seguenti parametri: nome stack per identificare il tuo nuovo stack, zona di disponibilità in cui si desidera eseguire lo stack e la coppia di chiavi che è possibile utilizzare per avviare le istanze EC2. Quindi puoi utilizzare la chiave privata corrispondente per accedere alle istanze EC2 tramite SSH.

   guardduty-tester.template richiede circa 10 minuti per l'esecuzione e il completamento. Crea il tuo ambiente e copia guardduty_tester.sh sulla tua istanza EC2 tester.

3. Nella AWS CloudFormation console, scegli la casella di controllo accanto al tuo nuovo running stack. AWS CloudFormation Nel set di schede visualizzato, selezionare la scheda Output. Nota che gli indirizzi IP assegnati al bastion host a al tester dell'istanza EC2. Hai bisogno di entrambi questi indirizzi IP per poter accedere alle istanze EC2 tester tramite SSH.

4. Crea la seguente voce nel file ~/.ssh/config per accedere all'istanza attraverso l'host bastione.

   ```
   Host bastion
           HostName {Elastic IP Address of Bastion}
           User ec2-user
           IdentityFile ~/.ssh/{your-ssh-key.pem}
   Host tester
           ForwardAgent yes
           HostName {Local IP Address of RedTeam Instance}
           User ec2-user
           IdentityFile ~/.ssh/{your-ssh-key.pem}
           ProxyCommand ssh bastion nc %h %p
           ServerAliveInterval 240
   ```

   Ora puoi chiamare $ ssh tester per accedere alla tua istanza EC2 di destinazione. Per ulteriori informazioni sulla configurazione e la connessione alle istanze EC2 tramite bastion hosts,

consulta https://aws.amazon.com/blogs/security/ - -/. securely-connect-to-linux instances-running-in-a private-amazon-vpc

5. Dopo esserti connesso all'istanza EC2 tester, esegui guardduty_tester.sh per avviare l'interazione tra il tester e le istanze EC2 bersaglio, simulare gli attacchi e generare risultati. GuardDuty

Livelli di gravità dei GuardDuty risultati

A ogni GuardDuty rilevazione è assegnato un livello di gravità e un valore che riflettono il rischio potenziale che la scoperta potrebbe comportare per la rete, secondo quanto stabilito dai nostri tecnici di sicurezza. Il valore della gravità può rientrare ovunque nell'intervallo da 1,0 a 8,9, con valori più alti che indicano un rischio maggiore per la sicurezza. Per aiutarti a determinare una risposta a un potenziale problema di sicurezza evidenziato da un risultato GuardDuty , suddividi questo intervallo in livelli di gravità alto, medio e basso.

> **Note**
>
> I valori 0 e quelli compresi tra 9,0 e 10,0 sono riservati per l'utilizzo futuro.

Di seguito sono riportati i livelli e i valori di gravità attualmente definiti per i GuardDuty risultati, nonché le raccomandazioni generali per ciascuno di essi:

Livello di gravità	Intervallo di valori
Elevate	7,0 - 8,9
Il livello "alto" indica che una risorsa (ad es. un'istanza EC2 o un set di credenziali di accesso di un utente IAM) è compromessa e che è attivamente utilizzata per scopi non autorizzati. Si consiglia di considerare prioritario qualsiasi problema di sicurezza di individuazione di gravità elevata e di adottare misure immediate per prevenire un ulteriore utilizzo non autorizzato delle risorse. Ad esempio, ripulire la tua istanza EC2 o terminarla oppure ruotare le credenziali IAM. Per ulteriori dettagli, vedere Procedure di correzione .	
Medio	4,0 - 6,9

Livello di gravità	Intervallo di valori
Un livello di gravità medio indica un'attività sospetta che si discosta dal comportamento normalmente osservato e, a seconda del caso d'uso, può essere indicativa di una compromissione delle risorse. Ti consigliamo di esaminare le risorse coinvolte appena possibile. I passaggi di correzione variano in base alla risorsa e alla famiglia Ricerca, ma in generale, dovresti verificare che l'attività sia autorizzata e coerente con il tuo caso d'uso. Se non è possibile identificare la causa o confermar e che l'attività è stata autorizzata, è necessario considerare la risorsa compromessa e seguire le Procedure di correzione per proteggere la risorsa. Ecco alcune cose da considerare quando si esamina una ricerca di livello medio: • Controlla se un utente autorizzato ha installato un nuovo software che ha modificato il comportamento di una risorsa (ad esempio, consentito un traffico da alto a normale o abilitato le comunicazioni su una nuova porta). • Controlla se un utente autorizzato ha modificato le impostazioni del pannello di controllo, per esempio, o ha cambiato le impostazioni del gruppo di sicurezza • Esegui una scansione antivirus sulla risorsa coinvolta per rilevare il software non autorizzato. • Verifica le autorizzazioni collegate a ruolo, utente, gruppi o un set di credenziali IAM coinvolti. Queste potrebbero essere modificate o ruotate.	
Bassa	1,0 - 3,9
Un livello di gravità basso indica un tentativo di attività sospetta che non ha compromesso la rete, ad esempio una scansione della porta o un tentativo di intrusione non riuscito. Non vi è alcuna operazione consigliata immediata, ma vale la pena prendere nota di queste informazioni in quanto ciò potrebbe indicare che qualcuno sta cercando punti deboli nella rete.	

GuardDuty ricerca dell'aggregazione

Tutti i risultati sono dinamici, il che significa che, se GuardDuty rileva una nuova attività correlata allo stesso problema di sicurezza, aggiornerà il risultato originale con le nuove informazioni, invece di generare un nuovo risultato. Questo comportamento consente di identificare i problemi in corso senza

dover esaminare più report simili e riduce il rumore complessivo causato da problemi di sicurezza di cui sei già a conoscenza.

Ad esempio, per un esito `UnauthorizedAccess:EC2/SSHBruteForce`, più tentativi di accesso contro l'istanza verranno aggregati allo stesso ID esito, aumentando il numero di conteggio nei dettagli dell'esito. Questo perché il rilevamento rappresenta un singolo problema di sicurezza con l'istanza che indica che la porta SSH sull'istanza non è adeguatamente protetta contro questo tipo di attività. Tuttavia, se GuardDuty rileva un'attività di accesso SSH rivolta a una nuova istanza nell'ambiente, creerà una nuova scoperta con un ID di ricerca univoco per avvisare l'utente del fatto che esiste un problema di sicurezza associato alla nuova risorsa.

Quando un esito viene aggregato, viene aggiornato con le informazioni relative all'ultima occorrenza di tale attività, il che significa che nell'esempio precedente se la tua istanza è la destinazione di un tentativo di forza bruta da un nuovo attore, i dettagli dell'esito verranno aggiornati per riflettere l'IP remoto dell'origine più recente e le precedenti informazioni saranno sostituite. Le informazioni complete sui singoli tentativi di attività saranno ancora disponibili nei tuoi log di flusso CloudTrail o in VPC.

I criteri che avvisano GuardDuty di generare un nuovo risultato invece di aggregarne uno esistente dipendono dal tipo di risultato. I criteri di aggregazione per ogni tipo di ricerca sono determinati dai nostri tecnici di sicurezza per offrirti la migliore panoramica dei problemi di sicurezza distinti all'interno del tuo account.

Individuazione e analisi dei risultati GuardDuty

Utilizza la procedura seguente per visualizzare e analizzare i GuardDuty risultati.

1. Aprire la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Scegliere Risultati e quindi scegliere un risultato specifico per visualizzarne i dettagli.

   I dettagli per ogni esito variano a seconda del tipo di esito, delle risorse coinvolte e della natura dell'attività. Per ulteriori informazioni sui campi di ricerca disponibili, vedere Dettagli degli esiti.
3. (Facoltativo) Se desideri archiviare un esito, selezionalo dall'elenco degli esiti e seleziona il menu Operazioni. Quindi scegli Archivia.

   Gli esiti archiviati possono essere visualizzati scegliendo Archiviati dall'elenco a discesa Attuali.

Attualmente GuardDuty gli utenti che accedono agli account dei GuardDuty membri non possono archiviare i risultati.

> **Important**
>
> Se si archivia una ricerca manualmente utilizzando la procedura qui sopra, tutte le successive occorrenze di questo risultato (generato dopo l'archiviazione) vengono aggiunte all'elenco dei risultati disponibili. Per non visualizzare mai questo risultato nell'elenco corrente, è possibile archiviarlo automaticamente. Per ulteriori informazioni, consulta Regole di eliminazione.

4. Per archiviare o scaricare un risultato, selezionarlo dall'elenco dei risultati, quindi scegliere il menu Operazioni. Quindi scegliere Esporta. Quando si esporta una ricerca, è possibile visualizzare l'intero documento in formato JSON.

> **Note**
>
> In alcuni casi, GuardDuty si rende conto che alcuni risultati sono falsi positivi dopo che sono stati generati. GuardDuty fornisce un campo Confidence nel codice JSON del risultato e ne imposta il valore su zero. In questo modo GuardDuty saprai che puoi tranquillamente ignorare tali risultati.

Tipi di esiti

Per informazioni sulle modifiche importanti ai tipi di risultati, inclusi i tipi di GuardDuty risultati appena aggiunti o ritirati, vedere. Cronologia dei documenti per Amazon GuardDuty

Per informazioni sui tipi di esiti che sono stati ritirati, consulta Tipi di esiti ritirati.

GuardDuty Tipi di ricerca EC2

Gli esiti seguenti sono specifici per le risorse Amazon EC2 e hanno sempre un Tipo risorsa di `Instance`. La gravità e i dettagli degli esiti variano in base al ruolo risorsa, che indica se la risorsa EC2 è stata la destinazione di attività sospette o l'attore che le ha eseguite.

Gli esiti qui elencati includono le origini dati e i modelli utilizzati per generare quel tipo di esito. Per ulteriori informazioni sulle origini dati e sui modelli, consulta Origini dati fondamentali.

> **Note**
>
> Per alcuni esiti EC2 potrebbero mancare i dettagli dell'istanza se quest'ultima è già stata terminata o se la chiamata API sottostante faceva parte di una chiamata API tra regioni originata da un'istanza EC2 in una regione diversa.

Per tutti gli esiti EC2, ti consigliamo di esaminare la risorsa in questione per determinare se si comporta nel modo previsto. Se l'attività è autorizzata, puoi utilizzare le regole di eliminazione o gli elenchi di indirizzi IP affidabili per prevenire notifiche false positive per quella risorsa. Se l'attività non è prevista, la best practice di sicurezza consiste nel presupporre che l'istanza sia stata compromessa e intraprendere le azioni dettagliate in Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Argomenti

- 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/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

Un'istanza EC2 esegue una query su un IP associato a un server di comando e controllo noto.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza elencata all'interno del tuo ambiente AWS esegue una query su un IP associato a un server di comando e controllo (C&C) noto. L'istanza elencata potrebbe essere compromessa. I server di comando e controllo sono computer che inviano comandi ai membri di una botnet.

Una botnet è una raccolta di dispositivi connessi a Internet, come PC, server, dispositivi mobili e dispositivi Internet of Things, che sono infettati e controllati da un tipo comune di malware. Le botnet sono spesso utilizzate per distribuire malware e rubare informazioni sensibili, ad esempio i numeri di carte di credito. A seconda dello scopo e della struttura della botnet, il server C&C potrebbe anche inviare comandi per lanciare un attacco DDoS (Distributed Denial of Service).

> **Note**
>
> Se l'IP su cui viene eseguita una query è correlato a log4j, determinati campi dell'esito associato includeranno i valori seguenti:
>
> - Servizio. Informazioni aggiuntive. threatListName = Amazon
> - service.additionalInfo.threatName = Log4j Related

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Backdoor:EC2/C&CActivity.B!DNS

Un'istanza EC2 esegue una query su un nome di dominio associato a un server di comando e controllo noto.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza elencata all'interno del tuo ambiente AWS esegue una query su un nome di dominio associato a un server di comando e controllo (C&C) noto. L'istanza elencata potrebbe essere compromessa. I server di comando e controllo sono computer che inviano comandi ai membri di una botnet.

Una botnet è una raccolta di dispositivi connessi a Internet, come PC, server, dispositivi mobili e dispositivi Internet of Things, che sono infettati e controllati da un tipo comune di malware. Le botnet sono spesso utilizzate per distribuire malware e rubare informazioni sensibili, ad esempio i numeri di carte di credito. A seconda dello scopo e della struttura della botnet, il server C&C potrebbe anche inviare comandi per lanciare un attacco DDoS (Distributed Denial of Service).

> **Note**
>
> Se il nome di dominio su cui è stata eseguita la query è relativo a log4j, i campi dell'esito associato includeranno i valori seguenti:
>
> - Servizio. Informazioni aggiuntive. threatListName = Amazon
> - service.additionalInfo.threatName = Log4j Related

> **Note**
>
> Per verificare come GuardDuty genera questo tipo di risultato, puoi effettuare una richiesta DNS dalla tua istanza (utilizzando `dig` per Linux o `nslookup` per Windows) su un dominio `guarddutyc2activityb.com` di test.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Backdoor:EC2/DenialOfService.Dns

Un'istanza EC2 si sta comportando in un modo che potrebbe indicare che viene utilizzata per eseguire un attacco Denial of Service (DoS) utilizzando il protocollo DNS.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata all'interno del tuo ambiente AWS genera un grande volume di traffico DNS in uscita. Ciò può indicare che l'istanza elencata è compromessa e viene utilizzata per eseguire attacchi denial-of-service (DoS) utilizzando il protocollo DNS.

> **Note**
>
> Questo risultato rileva attacchi DoS solo contro indirizzi IP instradabili pubblicamente, che sono gli obiettivi principali degli attacchi DoS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Backdoor:EC2/DenialOfService.Tcp

Un'istanza EC2 si sta comportando in un modo che potrebbe indicare che viene utilizzata per eseguire un attacco Denial of Service (DoS) utilizzando il protocollo TCP.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata all'interno del tuo ambiente AWS genera un grande volume di traffico TCP in uscita. Ciò può indicare che l'istanza è compromessa e viene utilizzata per eseguire attacchi denial-of-service (DoS) utilizzando il protocollo TCP.

> **Note**
>
> Questo risultato rileva attacchi DoS solo contro indirizzi IP instradabili pubblicamente, che sono gli obiettivi principali degli attacchi DoS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Backdoor:EC2/DenialOfService.Udp

Un'istanza EC2 si sta comportando in un modo che potrebbe indicare che viene utilizzata per eseguire un attacco Denial of Service (DoS) utilizzando il protocollo UDP.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata all'interno del tuo ambiente AWS genera un grande volume di traffico UDP in uscita. Ciò può indicare che l'istanza elencata è compromessa e viene utilizzata per eseguire attacchi denial-of-service (DoS) utilizzando il protocollo UDP.

> **Note**
>
> Questo risultato rileva attacchi DoS solo contro indirizzi IP instradabili pubblicamente, che sono gli obiettivi principali degli attacchi DoS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

Un'istanza EC2 si sta comportando in un modo che potrebbe indicare che viene utilizzata per eseguire un attacco Denial of Service (DoS) utilizzando il protocollo UDP sulla porta TCP.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata all'interno del tuo ambiente AWS genera un grande volume di traffico UDP in uscita indirizzato a una porta utilizzata di solito per le comunicazioni TCP. Ciò può indicare che l'istanza elencata è compromessa e viene utilizzata per eseguire attacchi denial-of-service (DoS) utilizzando il protocollo UDP su una porta TCP.

> **Note**
>
> Questo risultato rileva attacchi DoS solo contro indirizzi IP instradabili pubblicamente, che sono gli obiettivi principali degli attacchi DoS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Backdoor:EC2/DenialOfService.UnusualProtocol

Un'istanza EC2 si sta comportando in un modo che potrebbe indicare che viene utilizzata per eseguire un attacco Denial of Service (DoS) utilizzando un protocollo insolito.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS genera un grande volume di traffico in uscita da un tipo di protocollo insolito che normalmente non è utilizzato dalle istanze EC2, ad esempio, l'Internet Group Management Protocol. Ciò può indicare che l'istanza è compromessa e viene utilizzata per eseguire attacchi denial-of-service (DoS) utilizzando un protocollo insolito. Questo risultato rileva attacchi DoS solo contro indirizzi IP instradabili pubblicamente, che sono gli obiettivi principali degli attacchi DoS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Backdoor:EC2/Spambot

Un'istanza EC2 presenta un comportamento insolito in quanto comunica con un host remoto sulla porta 25.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS comunica con un host remoto sulla porta 25. Questo comportamento è inusuale in quanto l'istanza EC2 non ha mai comunicato sulla porta 25 in precedenza. La porta 25 è tradizionalmente utilizzata dai server di posta per le comunicazioni SMTP. Questo risultato indica che l'istanza EC2 potrebbe essere compromessa per l'uso nell'invio di spam.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Behavior:EC2/NetworkPortUnusual

Un'istanza EC2 sta comunicando con un host remoto su una porta server inusuale.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS si comporta in un modo che differisce dalla linea di base stabilita. Questa istanza EC2 non ha mai comunicato su questa porta remota in precedenza.

> **Note**
>
> Se l'istanza EC2 ha comunicato sulla porta 389 o sulla porta 1389, la gravità dell'esito associata verrà modificata in "alta" e i campi dell'esito includeranno il valore seguente:
>
> - service.additionalInfo.context = Possible log4j callback

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Behavior:EC2/TrafficVolumeUnusual

Un'istanza EC2 sta generando un volume di traffico di rete insolitamente elevato verso un host remoto.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS si comporta in un modo che differisce dalla linea di base stabilita. L'istanza EC2 non ha mai inviato una tale quantità di traffico a questo host remoto in precedenza.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

CryptoCurrency:EC2/BitcoinTool.B

Un'istanza EC2 sta eseguendo una query su un indirizzo IP associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS esegue una query su un indirizzo IP associato a un'attività correlata a Bitcoin o a un'altra criptovaluta. Il Bitcoin è una criptovaluta e un sistema di pagamento digitale utilizzato in tutto il mondo che può essere scambiato con altre valute, prodotti e servizi. Il Bitcoin è una ricompensa per il mining di Bitcoin ed è molto ricercato dagli autori delle minacce.

Raccomandazioni per la correzione:

Se utilizzi questa istanza EC2 per estrarre o gestire criptovaluta o se questa istanza è altrimenti coinvolta nell'attività di blockchain, questo esito potrebbe essere un'attività prevista per il tuo ambiente. Se questo è il caso del tuo ambiente AWS, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `CryptoCurrency:EC2/BitcoinTool.B`. Il secondo criterio di filtro dovrebbe essere l'ID istanza dell'istanza coinvolta nell'attività di blockchain. Per ulteriori informazioni sulla creazione di regole di soppressione, vedere Regole di eliminazione.

Se questa attività non è prevista, è probabile che l'istanza sia compromessa, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

CryptoCurrency:EC2/BitcoinTool.B!DNS

Un'istanza EC2 sta eseguendo una query su un nome di dominio associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS esegue una query su un nome di dominio associato a un'attività correlata a Bitcoin o a un'altra criptovaluta. Il Bitcoin è una criptovaluta e un sistema di pagamento digitale utilizzato in tutto il mondo che può essere scambiato

con altre valute, prodotti e servizi. Il Bitcoin è una ricompensa per il mining di Bitcoin ed è molto ricercato dagli autori delle minacce.

Raccomandazioni per la correzione:

Se utilizzi questa istanza EC2 per estrarre o gestire criptovaluta o se questa istanza è altrimenti coinvolta nell'attività di blockchain, questo esito potrebbe essere un'attività prevista per il tuo ambiente. Se questo è il caso del tuo ambiente AWS, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `CryptoCurrency:EC2/BitcoinTool.B!DNS`. Il secondo criterio di filtro dovrebbe essere l'ID istanza dell'istanza coinvolta nell'attività di blockchain. Per ulteriori informazioni sulla creazione di regole di soppressione, vedere Regole di eliminazione.

Se questa attività non è prevista, è probabile che l'istanza sia compromessa, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

DefenseEvasion:EC2/UnusualDNSResolver

Un'istanza Amazon EC2 comunica con un resolver DNS pubblico insolito.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza Amazon EC2 elencata nel tuo ambiente AWS si comporta in un modo che differisce dal comportamento di base. L'istanza EC2 in questione non ha alcuna storia recente di comunicazioni con questo resolver DNS pubblico. Il campo Unusual nel pannello dei dettagli di ricerca della GuardDuty console può fornire informazioni sul resolver DNS richiesto.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

DefenseEvasion:EC2/UnusualDoHActivity

Un'istanza Amazon EC2 esegue una comunicazione DNS su HTTPS (DoH) insolita.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza Amazon EC2 elencata all'interno del tuo ambiente AWS si comporta in un modo che differisce dalla linea di base stabilita. L'istanza EC2 in questione non ha alcuna storia recente di comunicazioni DNS su HTTPS (DoH) con questo server DoH pubblico. Il campo Insolito nei dettagli degli esiti può fornire informazioni sul server DoH su cui è stata effettuata la query.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

DefenseEvasion:EC2/UnusualDoTActivity

Un'istanza Amazon EC2 esegue una comunicazione DNS su TLS (DoT) insolita.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS si comporta in un modo che differisce dalla linea di base stabilita. L'istanza EC2 in questione non ha alcuna storia recente di comunicazioni DNS su TLS (DoT) con questo server DoT pubblico. Il campo Insolito nel pannello dei dettagli dell'esito può fornire informazioni sul server DoT su cui è stata effettuata la query.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Impact:EC2/AbusedDomainRequest.Reputation

Un'istanza EC2 esegue una query su un nome di dominio a bassa reputazione associato a domini noti in abuso.

Gravità predefinita: media

- Origine dati: log DNS

Questo esito segnala che l'istanza Amazon EC2 elencata all'interno del tuo ambiente AWS esegue una query su un nome di dominio a bassa reputazione associato a domini o indirizzi IP noti in abuso. Esempi di domini in abuso sono i nomi di dominio di primo livello (TLD) e i nomi di dominio di secondo livello (2LD) che offrono registrazioni gratuite di sottodomini e provider DNS dinamici. Gli autori delle minacce tendono a utilizzare questi servizi per registrare domini gratuitamente o a basso costo. I domini a bassa reputazione di questa categoria possono anche essere domini scaduti che vengono sostituiti con l'indirizzo IP di parcheggio di un registrar e quindi potrebbero non essere più attivi. Un IP di parcheggio è il luogo in cui un registrar indirizza il traffico verso domini che non sono stati collegati ad alcun servizio. L'istanza Amazon EC2 elencata potrebbe essere compromessa poiché gli autori delle minacce utilizzano comunemente questi registrar o servizi per la distribuzione di malware e C&C.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Impact:EC2/BitcoinDomainRequest.Reputation

Un'istanza EC2 esegue una query su un nome di dominio a bassa reputazione associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza Amazon EC2 elencata all'interno del tuo ambiente AWS esegue una query su un nome di dominio a bassa reputazione associato a un'attività correlata a Bitcoin o a un'altra criptovaluta. Il Bitcoin è una criptovaluta e un sistema di pagamento digitale utilizzato in tutto il mondo che può essere scambiato con altre valute, prodotti e servizi. Il Bitcoin è una ricompensa per il mining di Bitcoin ed è molto ricercato dagli autori delle minacce.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

Raccomandazioni per la correzione:

Se utilizzi questa istanza EC2 per estrarre o gestire criptovaluta o se questa istanza è altrimenti coinvolta nell'attività di blockchain, questo esito potrebbe rappresentare un'attività prevista per il tuo ambiente. Se questo è il caso del tuo ambiente AWS, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `Impact:EC2/BitcoinDomainRequest.Reputation`. Il secondo criterio di filtro dovrebbe essere l'ID istanza dell'istanza coinvolta nell'attività di blockchain. Per ulteriori informazioni sulla creazione di regole di soppressione, vedere Regole di eliminazione.

Se questa attività non è prevista, è probabile che l'istanza sia compromessa, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Impact:EC2/MaliciousDomainRequest.Reputation

Un'istanza EC2 esegue una query su un dominio a bassa reputazione associato a domini dannosi noti.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza Amazon EC2 elencata all'interno del tuo ambiente AWS esegue una query su un nome di dominio a bassa reputazione associato a domini o indirizzi IP dannosi noti. Ad esempio, i domini possono essere associati a un indirizzo IP sinkhole noto. I domini sinkhole sono domini che sono stati precedentemente controllati da un autore di minacce e se vengono inoltrate richieste a questi domini può significare che l'istanza è compromessa. Questi domini possono anche essere correlati a campagne dannose note o algoritmi di generazione di domini.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Impact:EC2/PortSweep

Su un gran numero di indirizzi IP è in corso il probing di una porta da parte di un'istanza EC2.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS effettua il probing di una porta su un gran numero di indirizzi IP instradabili pubblicamente. Questo tipo di attività viene in genere utilizzato per trovare host vulnerabili da sfruttare. Nel pannello dei dettagli di ricerca della GuardDuty console, viene visualizzato solo l'indirizzo IP remoto più recente

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Impact:EC2/SuspiciousDomainRequest.Reputation

Un'istanza EC2 esegue una query su un nome di dominio a bassa reputazione di natura sospetta a causa della sua età o della scarsa popolarità.

Gravità predefinita: bassa

- Origine dati: log DNS

Questo esito segnala che l'istanza Amazon EC2 elencata nel tuo ambiente AWS esegue una query su un nome di dominio a bassa reputazione sospettato di essere dannoso. Abbiamo notato che le caratteristiche di questo dominio sono coerenti con i domini dannosi osservati in precedenza, ma il nostro modello di reputazione non è stato in grado di collegarlo in modo definitivo a una minaccia nota. Questi domini vengono in genere osservati per la prima volta o ricevono una quantità di traffico ridotta.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Impact:EC2/WinRMBruteForce

Un'istanza EC2 esegue un attacco di forza bruta di Windows Remote Management in uscita.

Gravità predefinita: bassa*

> **Note**
>
> La gravità di questo esito è bassa se l'istanza EC2 era la destinazione di un attacco di forza bruta. La gravità di questo esito è alta se l'istanza EC2 è l'attore viene utilizzato per eseguire l'attacco di forza bruta.

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS esegue un attacco di forza bruta di Windows Remote Management (WinRM) volto a ottenere l'accesso al servizio Windows Remote Management su sistemi basati su Windows.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Recon:EC2/PortProbeEMRUnprotectedPort

Una porta non protetta EMR di un'istanza EC2 è sottoposta a probing da parte di un host dannoso noto.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo risultato indica che una porta sensibile relativa all'EMR sull'istanza EC2 elencata che fa parte di un cluster nel AWS tuo ambiente non è bloccata da un gruppo di sicurezza, da una lista di controllo degli accessi (ACL) o da un firewall on-host come Linux IPTables. Questa scoperta indica inoltre che scanner noti su Internet stanno sondando attivamente questa porta. Le porte che possono attivare questo esito, ad esempio la porta 8088 (porta dell'interfaccia utente Web YARN), potrebbero potenzialmente essere utilizzate per l'esecuzione di codice in modalità remota.

Raccomandazioni per la correzione:

Ti consigliamo di bloccare l'accesso aperto alle porte su cluster da Internet e limitare l'accesso solo a indirizzi IP specifici che richiedono l'accesso a queste porte. Per ulteriori informazioni, consultare Gruppi di sicurezza per cluster EMR.

Recon:EC2/PortProbeUnprotectedPort

Una porta non protetta di un'istanza EC2 è sottoposta a probing da parte di un host dannoso noto.

Gravità predefinita: bassa*

> **Note**
>
> La gravità predefinita di questi esiti è bassa. Tuttavia, se la porta che viene esaminata viene utilizzata da Elasticsearch (9200 o 9300), la gravità del risultato è elevata.

- Origine dati: log di flusso VPC

Questo esito segnala che una porta sull'istanza EC2 elencata nel tuo ambiente AWS non è bloccata da un gruppo di sicurezza, una lista di controllo degli accessi (ACL) o un firewall su host, ad esempio, Linux IPTables, e che è sottoposta attivamente a probing da parte di scanner noti.

Se la porta non protetta identificata è 22 o 3389 e si utilizzano queste porte per connettersi all'istanza, è comunque possibile limitare l'esposizione consentendo l'accesso a queste porte solo agli indirizzi

IP dello spazio degli indirizzi IP della rete aziendale. Per limitare l'accesso alla porta 22 su Linux, consulta Authorizing Inbound Traffic for Your Linux Instance. Per limitare l'accesso alla porta 3389 su Windows, consulta Authorizing Inbound Traffic for Your Windows Instances.

GuardDuty non genera questo risultato per le porte 443 e 80.

Raccomandazioni per la correzione:

Tuttavia, ci possono essere casi in cui le istanze sono intenzionalmente esposte, ad esempio se ospitano server web. Se questo è il caso del tuo ambiente AWS, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `Recon:EC2/PortProbeUnprotectedPort`. Il secondo criterio di filtro deve corrispondere all'istanza o alle istanze che fungono da bastion host. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda del criterio identificabile con le istanze che ospitano questi strumenti. Per ulteriori informazioni sulla creazione di regole di eliminazione, consulta Regole di eliminazione.

Se questa attività non è prevista, è probabile che l'istanza sia compromessa, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Recon:EC2/Portscan

Un'istanza EC2 sta eseguendo la scansione delle porte in uscita verso un host remoto.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS è coinvolta in un possibile attacco port scan in quanto sta effettuando più tentativi di connessione a diverse porte in un breve periodo di tempo. Lo scopo di un attacco port scan è di individuare le porte aperte per determinare quali servizi sono in esecuzione sulla macchina e per identificarne il sistema operativo.

Raccomandazioni per la correzione:

Questo esito può essere un falso positivo se nel tuo ambiente vengono implementate applicazioni di valutazione della vulnerabilità su istanze EC2. Queste applicazioni, infatti, eseguono scansioni

delle porte per avvisarti in caso di porte aperte configurate in modo errato. Se questo è il caso del tuo ambiente AWS, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `Recon:EC2/Portscan`. Il secondo criterio di filtro dovrebbe corrispondere all'istanza o alle istanze che ospitano questi strumenti di valutazione della vulnerabilità. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda dei criteri identificabili con le istanze che ospitano questi strumenti. Per ulteriori informazioni sulla creazione di regole di eliminazione, consulta Regole di eliminazione.

Se questa attività non è prevista, è probabile che l'istanza sia compromessa, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Trojan:EC2/BlackholeTraffic

Un'istanza EC2 sta tentando di comunicare con un indirizzo IP di un host remoto che è un noto buco nero.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 nel tuo ambiente AWS potrebbe essere compromessa in quanto tenta di comunicare con l'indirizzo IP di un buco nero (o sinkhole). I buchi neri sono zone della rete dove il traffico in entrata e in uscita viene eliminato silenziosamente senza che l'origine venga informata del mancato recapito dei dati al destinatario. L'indirizzo IP di un buco nero designa un computer host non in esecuzione o un indirizzo a cui non è stato assegnato alcun host.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Trojan:EC2/BlackholeTraffic!DNS

Un'istanza EC2 sta eseguendo una query su un nome di dominio che è reindirizzato a un indirizzo IP di un buco nero.

Gravità predefinita: media

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS potrebbe essere compromessa in quanto esegue una query su un nome di dominio che è reindirizzato all'indirizzo IP di un buco nero. I buchi neri sono zone della rete dove il traffico in entrata e in uscita viene eliminato silenziosamente senza che l'origine venga informata del mancato recapito dei dati al destinatario.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Trojan:EC2/DGADomainRequest.B

Un'istanza EC2 sta eseguendo una query su domini generati da algoritmi. Tali domini sono in genere utilizzati da malware e potrebbero essere un'indicazione di un'istanza EC2 compromessa.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 nel tuo ambiente AWS tenta di eseguire una query su domini DGA. L'istanza EC2 potrebbe essere compromessa.

I DGA sono utilizzati periodicamente per generare un gran numero di nomi di dominio che possono essere utilizzati come punti di incontro con i relativi server di comando e controllo (C&C). I server di comando e controllo sono computer che inviano comandi a membri di una botnet, ovvero una raccolta di dispositivi connessi a Internet infettati e controllati da un tipo comune di malware. Il numero elevato di punti di rendez-vous potenziali rende difficile l'arresto delle botnet in quanto i computer infettati tentano di contattare quotidianamente alcuni di questi nomi di dominio per ricevere aggiornamenti o comandi.

> **Note**
>
> L'esito è basato sull'analisi dei nomi di dominio tramite un'euristica avanzata e può quindi identificare nuovi domini DGA che non sono presenti nei feed di intelligence sulle minacce.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Trojan:EC2/DGADomainRequest.C!DNS

Un'istanza EC2 sta eseguendo una query su domini generati da algoritmi. Tali domini sono in genere utilizzati da malware e potrebbero essere un'indicazione di un'istanza EC2 compromessa.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 nel tuo ambiente AWS tenta di eseguire una query su domini DGA. L'istanza EC2 potrebbe essere compromessa.

I DGA sono utilizzati periodicamente per generare un gran numero di nomi di dominio che possono essere utilizzati come punti di incontro con i relativi server di comando e controllo (C&C). I server di comando e controllo sono computer che inviano comandi a membri di una botnet, ovvero una raccolta di dispositivi connessi a Internet infettati e controllati da un tipo comune di malware. Il numero elevato di punti di rendez-vous potenziali rende difficile l'arresto delle botnet in quanto i computer infettati tentano di contattare quotidianamente alcuni di questi nomi di dominio per ricevere aggiornamenti o comandi.

> **Note**
>
> Questo risultato si basa su domini DGA noti tratti dai feed GuardDuty di intelligence sulle minacce.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Trojan:EC2/DNSDataExfiltration

Un'istanza EC2 sta eseguendo l'esfiltrazione di dati tramite query DNS.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS esegue un malware che utilizza query DNS per trasferire dati in uscita. Questo tipo di trasferimento di dati è indicativo di un'istanza compromessa e potrebbe comportare l'esfiltrazione di dati. Di solito, il traffico DNS non è bloccato dai firewall. Ad esempio, il malware in un'istanza EC2 compromessa può codificare i dati (ad esempio i numeri di carte di credito) in una query DNS e inviarli a un server DNS remoto controllato da un utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Trojan:EC2/DriveBySourceTraffic!DNS

Un'istanza EC2 sta eseguendo una query su un nome di dominio di un host remoto che è l'origine nota di attacchi di download drive-by.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS potrebbe essere compromessa in quanto esegue una query su un nome di dominio di un host remoto che è un'origine nota di attacchi di download drive-by. Si tratta di download di software non voluti da Internet che possono attivare l'installazione automatica di virus, spyware o malware.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Trojan:EC2/DropPoint

Un'istanza EC2 sta tentando di comunicare con un indirizzo IP di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS tenta di comunicare con l'indirizzo IP di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Trojan:EC2/DropPoint!DNS

Un'istanza EC2 sta eseguendo una query su un nome di dominio di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Gravità predefinita: media

- Origine dati: log DNS

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS esegue una query su un nome di dominio di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Trojan:EC2/PhishingDomainRequest!DNS

Un'istanza EC2 sta eseguendo una query su domini implicati in attacchi di phishing. L'istanza EC2 potrebbe essere compromessa.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che nel tuo ambiente AWS è presente un'istanza EC2 che tenta di eseguire una query su un dominio implicato in attacchi di phishing. I domini di phishing sono configurati da individui che fingono di essere un'istituzione legittima allo scopo di indurre gli utenti a fornire dati sensibili come informazioni personali, coordinate bancarie, informazioni di carte di credito e password. L'istanza EC2 potrebbe tentare di recuperare dati sensibili archiviati su un sito Web di phishing oppure di configurare un sito Web di phishing. L'istanza EC2 potrebbe essere compromessa.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

Un'istanza EC2 stabilisce connessioni a un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS comunica con un indirizzo IP incluso in un elenco minacce che hai caricato. In GuardDuty, un elenco di minacce è costituito da indirizzi IP dannosi noti. GuardDuty genera i risultati in base agli elenchi di minacce caricati. L'elenco delle minacce utilizzato per generare questo risultato verrà elencato nei dettagli del risultato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

UnauthorizedAccess:EC2/MetadataDNSRebind

Un'istanza EC2 esegue ricerche DNS che vengono risolte nel servizio di metadati dell'istanza.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS esegue una query su un dominio che restituisce l'indirizzo IP dei metadati EC2 (169.254.169.254). Una query DNS di questo tipo può indicare che l'istanza è la destinazione di una tecnica di rebinding DNS. Questa tecnica può essere utilizzata per ottenere metadati da un'istanza EC2, incluse le credenziali IAM a essa associate.

Il rebinding DNS implica l'inganno di un'applicazione in esecuzione sull'istanza EC2 per caricare i dati restituiti da un URL, dove il nome di dominio nell'URL si risolve nell'indirizzo IP dei metadati EC2 (169.254.169.254). In questo modo l'applicazione accede ai metadati EC2 e, possibilmente, li rende disponibili all'utente malintenzionato.

Puoi accedere ai metadati EC2 utilizzando il rebinding DNS solo se l'istanza EC2 esegue un'applicazione vulnerabile che consente l'iniezione di URL oppure se qualcuno accede all'URL in un browser Web in esecuzione sull'istanza EC2.

Raccomandazioni per la correzione:

In risposta a questo esito, devi valutare se è presente un'applicazione vulnerabile in esecuzione sull'istanza EC2 o se qualcuno ha utilizzato un browser per accedere al dominio identificato nell'esito. Se la causa principale è un'applicazione vulnerabile, è necessario correggere la vulnerabilità. Se qualcuno ha navigato nel dominio identificato, è necessario bloccare il dominio o impedire agli utenti di accedervi. Se ritieni che l'esito sia correlato a uno dei due casi precedenti, revoca la sessione associata all'istanza EC2.

Alcuni clienti AWS mappano intenzionalmente l'indirizzo IP dei metadati a un nome di dominio sui server DNS autorevoli. Se questo è il caso del tuo ambiente , ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `UnauthorizedAccess:EC2/MetaDataDNSRebind`. Il secondo criterio di filtro deve essere il dominio di richiesta DNS e il valore deve corrispondere al dominio mappato all'indirizzo IP dei

metadati (169.254.169.254). Per ulteriori informazioni sulla creazione di regole di soppressione, vedere Regole di eliminazione.

UnauthorizedAccess:EC2/RDPBruteForce

Un'istanza EC2 è stata implicata in attacchi forza bruta RDP.

Gravità predefinita: bassa*

> **Note**
>
> La gravità di questo esito è bassa se l'istanza EC2 era la destinazione di un attacco di forza bruta. La gravità di questo esito è alta se l'istanza EC2 è l'attore viene utilizzato per eseguire l'attacco di forza bruta.

- Origine dati: log di flusso VPC

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS è stata coinvolta in un attacco forza bruta che mirava a ottenere le password dei servizi RDP su sistemi basati su Windows. Ciò può indicare un accesso non autorizzato alle risorse AWS.

Raccomandazioni per la correzione:

Se il Ruolo risorsa dell'istanza è `ACTOR`, significa che l'istanza è stata utilizzata per eseguire gli attacchi di forza bruta RDP. A meno che questa istanza non abbia un motivo legittimo per contattare l'indirizzo IP elencato come `Target`, ti consigliamo di presumere che l'istanza sia stata compromessa e di intraprendere le azioni elencate in Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Se il Ruolo risorsa dell'istanza è `TARGET`, questo esito può essere risolto proteggendo la porta RDP, consentendo l'accesso solo agli IP affidabili tramite gruppi di sicurezza, ACL o firewall. Per ulteriori informazioni, consulta Suggerimenti per la protezione delle istanze EC2 (Linux).

UnauthorizedAccess:EC2/SSHBruteForce

Un'istanza EC2 è stata implicata in attacchi forza bruta SSH.

Gravità predefinita: bassa*

> **Note**
>
> La gravità di questo esito è bassa se un attacco di forza bruta è rivolto a una delle istanze EC2. La gravità di questo esito è alta se l'istanza EC2 viene utilizzata per eseguire l'attacco di forza bruta.

- Origine dati: log di flusso VPC

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS è stata coinvolta in un attacco forza bruta che mirava a ottenere le password dei servizi SSH su sistemi basati su Linux. Ciò può indicare un accesso non autorizzato alle risorse AWS.

> **Note**
>
> Questo risultato viene generato solo dal monitoraggio del traffico di sulla porta 22. Se i servizi SSH sono configurati per utilizzare altre porte, questo risultato non viene generato.

Raccomandazioni per la correzione:

Se la destinazione del tentativo di attacco forza bruta è un host bastione, questo comportamento potrebbe essere previsto per l'ambiente AWS. In questo caso, si consiglia di impostare una regola di eliminazione per questa individuazione. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `UnauthorizedAccess:EC2/SSHBruteForce`. Il secondo criterio di filtro deve corrispondere all'istanza o alle istanze che fungono da bastion host. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda del criterio identificabile con le istanze che ospitano questi strumenti. Per ulteriori informazioni sulla creazione di regole di eliminazione, consulta Regole di eliminazione.

Se questa attività non è prevista per il tuo ambiente e il Ruolo risorsa dell'istanza è `TARGET`, questo esito può essere risolto proteggendo la porta SSH, consentendo l'accesso solo a IP affidabili tramite

gruppi di sicurezza, ACL o firewall. Per ulteriori informazioni, consulta Suggerimenti per la protezione delle istanze EC2 (Linux).

Se il Ruolo risorsa dell'istanza è `ACTOR`, questo indica che l'istanza è stata utilizzata per eseguire gli attacchi di forza bruta SSH. A meno che questa istanza non abbia un motivo legittimo per contattare l'indirizzo IP elencato come `Target`, ti consigliamo di presumere che l'istanza sia stata compromessa e di intraprendere le azioni elencate in Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

UnauthorizedAccess:EC2/TorClient

L'istanza EC2 sta stabilendo connessioni a un Tor Guard o a un nodo Authority.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS stabilisce connessioni a un Tor Guard o a un nodo Authority. Tor è un software che consente la comunicazione anonima. I Tor Guard e i nodi fungono da gateway iniziali per una rete Tor. Questo traffico può indicare che l'istanza EC2 è stata compromessa e funge da client su una rete Tor. L'esito potrebbe indicare un accesso non autorizzato alle risorse AWS con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

UnauthorizedAccess:EC2/TorRelay

L'istanza EC2 sta stabilendo connessioni a una rete Tor come relay Tor.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS stabilisce connessioni a una rete Tor in un modo che suggerisce che funga da relè Tor. Tor è un software che consente la comunicazione

anonima. Tor aumenta l'anonimato della comunicazione inoltrando il traffico potenzialmente illecito del client da un relè Tor a un altro.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

GuardDuty Tipi di ricerca IAM

Gli esiti seguenti sono specifici per le entità IAM e le chiavi di accesso e avranno sempre un Tipo risorsa di `AccessKey`. La gravità e i dettagli degli esiti variano in base al tipo di esito.

Gli esiti qui elencati includono le origini dati e i modelli utilizzati per generare quel tipo di esito. Per ulteriori informazioni, consulta Origini dati fondamentali.

Per tutti gli esiti relativi a IAM, ti consigliamo di esaminare l'entità in questione e assicurarti che le relative autorizzazioni seguano la best practice del privilegio minimo. Se l'attività non è prevista, le credenziali potrebbero essere compromesse. Per informazioni su come correggere gli esiti, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Argomenti

- CredentialAccess:IAMUser/AnomalousBehavior
- DefenseEvasion:IAMUser/AnomalousBehavior
- 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
- 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/TorIPCaller

CredentialAccess:IAMUser/AnomalousBehavior

Un'API utilizzata per accedere a un AWS ambiente è stata richiamata in modo anomalo.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questo esito segnala che è stata osservata una richiesta API anomala nel tuo account. Questo esito può includere una singola richiesta API o una serie di richieste API correlate effettuate in prossimità da un'unica identità utente. L'API osservata è comunemente associata alla fase di accesso alle credenziali di un attacco, quando un avversario tenta di raccogliere password, nomi utente e chiavi di accesso per il tuo ambiente. Le API di questa categoria sono `GetPasswordData`, `GetSecretValue` e `GenerateDbAuthToken`.

Questa richiesta API è stata identificata come anomala dal modello GuardDuty di machine learning (ML) di rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta. Nei dettagli sui risultati sono disponibili le informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

DefenseEvasion:IAMUser/AnomalousBehavior

Un'API utilizzata per eludere le misure difensive è stata richiamata in modo anomalo.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questo esito segnala che è stata osservata una richiesta API anomala nel tuo account. Questo esito può includere una singola richiesta API o una serie di richieste API correlate effettuate in prossimità da un'unica identità utente. L'API osservata è comunemente associata a tattiche di evasione della difesa in cui un avversario cerca di coprire le proprie tracce e non essere rilevato. Le API di questa categoria sono in genere operazioni di eliminazione, disabilitazione o interruzione, come `DeleteFlowLogs`, `DisableAlarmActions` o `StopLogging`.

Questa richiesta API è stata identificata come anomala dal modello GuardDuty di machine learning (ML) di rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta. Nei dettagli sui risultati sono disponibili le informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Discovery:IAMUser/AnomalousBehavior

Un'API comunemente utilizzata per scovare le risorse è stata richiamata in modo anomalo.

Gravità predefinita: bassa

- Fonte dei dati: evento di gestione CloudTrail

Questo esito segnala che è stata osservata una richiesta API anomala nel tuo account. Questo esito può includere una singola richiesta API o una serie di richieste API correlate effettuate in prossimità da un'unica identità utente. L'API osservata è generalmente associata alla fase di scoperta di un attacco, quando un avversario raccoglie informazioni per determinare se l' AWS ambiente è suscettibile a un attacco più ampio. Le API di questa categoria sono in genere operazioni di recupero, descrizione o elenco, come `DescribeInstances`, `GetRolePolicy` o `ListAccessKeys`.

Questa richiesta API è stata identificata come anomala dal modello di machine learning (ML) GuardDuty di rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta. Nei dettagli sui risultati sono disponibili le informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Exfiltration:IAMUser/AnomalousBehavior

Un'API comunemente utilizzata per raccogliere dati da un AWS ambiente è stata richiamata in modo anomalo.

Gravità predefinita: alta

- Fonte dei dati: evento di gestione CloudTrail

Questo esito segnala che è stata osservata una richiesta API anomala nel tuo account. Questo esito può includere una singola richiesta API o una serie di richieste API correlate effettuate in prossimità da un'unica identità utente. L'API osservata è comunemente associata a tattiche di esfiltrazione in cui un avversario cerca di raccogliere dati dalla tua rete utilizzando pacchetti e crittografia per non essere rilevato. Le API per questo tipo di esiti sono solo operazioni di gestione, ossia piano di controllo (control-plane), e sono in genere correlate a S3, snapshot e database, come `PutBucketReplication`, `CreateSnapshot` o `RestoreDBInstanceFromDBSnapshot`.

Questa richiesta API è stata identificata come anomala dal modello GuardDuty di machine learning (ML) di rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta. Nei dettagli sui risultati sono disponibili le informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Impact:IAMUser/AnomalousBehavior

Un'API comunemente utilizzata per manomettere dati o processi in un AWS ambiente è stata richiamata in modo anomalo.

Gravità predefinita: alta

- Fonte dei dati: evento di gestione CloudTrail

Questo esito segnala che è stata osservata una richiesta API anomala nel tuo account. Questo esito può includere una singola richiesta API o una serie di richieste API correlate effettuate in prossimità da un'unica identità utente. L'API osservata è comunemente associata a tattiche di impatto con cui un avversario cerca di interferire con le operazioni e manipolare, interrompere o distruggere i dati del tuo account. Le API per questo tipo di esiti sono in genere operazioni di eliminazione, aggiornamento o put, come `DeleteSecurityGroup`, `UpdateUser` o `PutBucketPolicy`.

Questa richiesta API è stata identificata come anomala dal modello GuardDuty di machine learning (ML) di rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta. Nei dettagli sui risultati sono disponibili le informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

InitialAccess:IAMUser/AnomalousBehavior

Un'API comunemente utilizzata per ottenere l'accesso non autorizzato a un AWS ambiente è stata richiamata in modo anomalo.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questo esito segnala che è stata osservata una richiesta API anomala nel tuo account. Questo esito può includere una singola richiesta API o una serie di richieste API correlate effettuate in prossimità da un'unica identità utente. L'API osservata è comunemente associata alla fase di accesso iniziale di un attacco, quando un avversario tenta di accedere al tuo ambiente. Le API di questa categoria sono in genere operazioni di recupero token o di sessione, come `GetFederationToken`, `StartSession`, o `GetAuthorizationToken`.

Questa richiesta API è stata identificata come anomala dal modello GuardDuty di machine learning (ML) di rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta. Nei dettagli sui risultati sono disponibili le informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

PenTest:IAMUser/KaliLinux

Un'API è stata richiamata da una macchina Kali Linux.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questa scoperta ti informa che una macchina che esegue Kali Linux sta effettuando chiamate API utilizzando credenziali che appartengono all' AWS account elencato nel tuo ambiente. Kali Linux è uno noto strumento per l'esecuzione di test di intrusione utilizzato dai professionisti della sicurezza informatica per identificare le vulnerabilità nelle istanze EC2 che richiedono l'applicazione di patch. Gli aggressori utilizzano questo strumento anche per individuare i punti deboli della configurazione EC2 e ottenere l'accesso non autorizzato al tuo ambiente. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

PenTest:IAMUser/ParrotLinux

Un'API è stata richiamata da una macchina Parrot Security Linux.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questa scoperta indica che una macchina che esegue Parrot Security Linux sta effettuando chiamate API utilizzando credenziali che appartengono all' AWS account elencato nell'ambiente in uso. Parrot Security Linux è uno noto strumento per l'esecuzione di test di intrusione utilizzato dai professionisti della sicurezza informatica per identificare le vulnerabilità nelle istanze EC2 che richiedono l'applicazione di patch. Gli aggressori utilizzano questo strumento anche per individuare i punti deboli della configurazione EC2 e ottenere l'accesso non autorizzato all'ambiente in uso. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

PenTest:IAMUser/PentooLinux

Un'API è stata richiamata da una macchina Pentoo Linux.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questa scoperta ti informa che una macchina che esegue Pentoo Linux sta effettuando chiamate API utilizzando credenziali che appartengono all' AWS account elencato nel tuo ambiente. Pentoo Linux è uno noto strumento per l'esecuzione di test di intrusione utilizzato dai professionisti della sicurezza informatica per identificare le vulnerabilità nelle istanze EC2 che richiedono l'applicazione di patch. Gli aggressori utilizzano questo strumento anche per individuare i punti deboli della configurazione EC2 e ottenere l'accesso non autorizzato al tuo ambiente. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Persistence:IAMUser/AnomalousBehavior

Un'API comunemente utilizzata per mantenere l'accesso non autorizzato a un AWS ambiente è stata richiamata in modo anomalo.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questo esito segnala che è stata osservata una richiesta API anomala nel tuo account. Questo esito può includere una singola richiesta API o una serie di richieste API correlate effettuate in prossimità da un'unica identità utente. L'API osservata è comunemente associata a tattiche di persistenza in cui un avversario ha ottenuto l'accesso al tuo ambiente e cerca di mantenerlo. Le API di questa categoria sono in genere operazioni di creazione, importazione o modifica, come `CreateAccessKey`, `ImportKeyPair` o `ModifyInstanceAttribute`.

Questa richiesta API è stata identificata come anomala dal modello GuardDuty di machine learning (ML) di rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta. Nei dettagli sui risultati sono disponibili le informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Policy:IAMUser/RootCredentialUsage

Un'API è stata richiamata utilizzando le credenziali di accesso di un utente root.

Gravità predefinita: bassa

- Fonte dei dati: eventi di CloudTrail gestione o eventi relativi ai dati CloudTrail

Questo esito segnala che le credenziali di accesso dell'utente root dell' Account AWS elencato nel tuo ambiente vengono utilizzate per effettuare richieste ai servizi AWS . Si consiglia agli utenti di non utilizzare mai le credenziali di accesso dell'utente root per accedere ai servizi AWS . È invece necessario accedere AWS ai servizi utilizzando le credenziali temporanee con privilegi minimi di (STS). AWS Security Token Service Nelle situazioni in cui AWS STS non è supportato, consigliamo di utilizzare le credenziali dell'utente IAM. Per ulteriori informazioni, consulta Best Practice IAM.

> **Note**
>
> Se il rilevamento delle minacce di S3 è abilitato per l'account, questo esito può essere generato in risposta ai tentativi di eseguire operazioni del piano dati S3 sulle risorse S3 utilizzando le credenziali di accesso dell'utente root di Account AWS. La chiamata API utilizzata verrà elencata nei dettagli dell'esito. Se il rilevamento delle minacce di S3 non è abilitato, questo esito può essere attivato solo dalle API del log eventi. Per maggiori informazioni sul rilevamento delle minacce di S3, consulta Protezione S3.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

PrivilegeEscalation:IAMUser/AnomalousBehavior

Un'API comunemente utilizzata per ottenere autorizzazioni di alto livello per un AWS ambiente è stata richiamata in modo anomalo.

Gravità predefinita: media

- Fonte dei dati: eventi di gestione CloudTrail

Questo esito segnala che è stata osservata una richiesta API anomala nel tuo account. Questo esito può includere una singola richiesta API o una serie di richieste API correlate effettuate in prossimità da un'unica identità utente. L'API osservata è comunemente associata a tattiche di escalation dei privilegi in cui un avversario tenta di ottenere autorizzazioni di livello superiore per un ambiente. Le API di questa categoria in genere coinvolgono operazioni che modificano le policy, i ruoli e gli utenti IAM, come `AssociateIamInstanceProfile`, `AddUserToGroup` o `PutUserPolicy`.

Questa richiesta API è stata identificata come anomala dal modello ML (Anomaly GuardDuty Detection Machine Learning) di Anomaly Detection. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori della richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata e l'API specifica che è stata richiesta. Nei dettagli sui risultati sono disponibili le informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Recon:IAMUser/MaliciousIPCaller

Un'API è stata chiamata da un indirizzo IP dannoso noto.

Gravità predefinita: media

- Fonte dei dati: eventi di gestione CloudTrail

Questo esito segnala che un'operazione API in grado di elencare o descrivere le risorse AWS di un account all'interno del tuo ambiente è stata richiamata da un indirizzo IP incluso in un elenco minacce. Un utente malintenzionato può utilizzare credenziali rubate per eseguire questo tipo di ricognizione delle AWS risorse dell'utente al fine di trovare credenziali più preziose o determinare le funzionalità delle credenziali già in suo possesso.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Recon:IAMUser/MaliciousIPCaller.Custom

Un'API è stata chiamata da un indirizzo IP dannoso noto.

Gravità predefinita: media

- Fonte dei dati: eventi di gestione CloudTrail

Questo esito segnala che un'operazione API in grado di elencare o descrivere le risorse AWS di un account all'interno del tuo ambiente è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato. L'elenco delle minacce utilizzato sarà elencato nei dettagli del risultato. Un utente malintenzionato potrebbe utilizzare credenziali rubate per eseguire questo tipo di ricognizione delle AWS risorse dell'utente al fine di trovare credenziali più preziose o determinare le funzionalità delle credenziali già in suo possesso.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Recon:IAMUser/TorIPCaller

Un'API è stata chiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: media

- Fonte dei dati: eventi di gestione CloudTrail

Questo esito segnala che un'operazione API in grado di elencare o descrivere le risorse AWS di un account all'interno del tuo ambiente è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Un utente malintenzionato può usare Tor per mascherare la propria identità.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail la registrazione è stata disabilitata.

Gravità predefinita: bassa

- Fonte dei dati: eventi CloudTrail di gestione

Questa scoperta indica che una CloudTrail traccia all'interno AWS dell'ambiente in uso è stata disattivata. Può trattarsi di un tentativo di un utente malintenzionato di disabilitare la registrazione per eliminare le tracce della sua attività accedendo nel contempo alle risorse AWS per scopi dannosi. Questo risultato può essere generato dall'eliminazione o dall'aggiornamento riuscito di un trail Questo risultato può essere innescato anche dall'eliminazione riuscita di un bucket S3 che memorizza i log di un trail associato a. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Stealth:IAMUser/PasswordPolicyChange

La policy delle password dell'account è stata indebolita.

Gravità predefinita: bassa*

> **Note**
>
> La gravità di questo esito può essere bassa, media o alta a seconda della gravità delle modifiche apportate alla policy delle password.

- Fonte dei dati: eventi di gestione CloudTrail

La politica relativa alle password degli AWS account è stata indebolita nell'account elencato nell' AWS ambiente in uso. Ad esempio, è stata eliminata o aggiornata per richiedere un numero minore di caratteri, non richiedere simboli e numeri o per prolungare l'estensione del periodo di scadenza delle password. Questo risultato può essere causato anche dal tentativo di aggiornare o eliminare la politica relativa alle password AWS dell'account. La politica sulle password degli AWS account definisce le regole che regolano i tipi di password che possono essere impostati per gli utenti IAM. Un policy delle password indebolita consente la creazione di password facili da ricordare e potenzialmente più facili da indovinare, creando di fatto un rischio per la sicurezza.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

Molteplici connessioni riuscite alla console sono state osservate in tutto il mondo.

Gravità predefinita: media

- Fonte dei dati: eventi di gestione CloudTrail

Questo risultato segnala che molteplici connessioni riuscite alla console da parte dello stesso utente IAM sono state osservate simultaneamente in varie regioni geografiche. Questi modelli di localizzazione degli accessi anomali e rischiosi indicano un potenziale accesso non autorizzato alle risorse dell'utente. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

Credenziali create in modo esclusivo per un'istanza EC2 mediante un ruolo di avvio di istanze vengono utilizzate da un altro account all'interno di AWS.

Gravità predefinita: alta*

> **Note**
>
> La gravità predefinita di questi esiti è alta. Tuttavia, se l'API è stata richiamata da un account affiliato all' AWS ambiente in uso, la gravità è Media.

- Fonte dei dati: eventi di CloudTrail gestione o eventi relativi ai dati S3

Questo risultato ti informa quando le credenziali dell'istanza EC2 vengono utilizzate per richiamare le API da un indirizzo IP di proprietà di un AWS account diverso da quello su cui è in esecuzione l'istanza EC2 associata.

AWS non consiglia di ridistribuire le credenziali temporanee all'esterno dell'entità che le ha create (ad esempio, AWS applicazioni, EC2 o Lambda). Tuttavia, gli utenti autorizzati possono esportare le credenziali dalle proprie istanze EC2 per rendere legittime le chiamate API. Se il `remoteAccountDetails.Affiliated` campo è, `True` l'API è stata richiamata da un account associato al tuo ambiente. AWS Per escludere un potenziale attacco e verificare la legittimità delle attività, contatta l'utente IAM a cui queste credenziali sono assegnate.

> **Note**
>
> Se GuardDuty rileva l'attività continua di un account remoto, il relativo modello di machine learning (ML) la identificherà come un comportamento previsto. Pertanto, GuardDuty smetterà di generare questo risultato per l'attività da quell'account remoto. GuardDuty continuerà a generare risultati relativi a nuovi comportamenti provenienti da altri account remoti e rivaluterà gli account remoti appresi man mano che il comportamento cambia nel tempo.

Raccomandazioni per la correzione:

In risposta a questo esito, puoi utilizzare il seguente flusso di lavoro per determinare una linea d'azione:

1. Identifica l'account remoto coinvolto tramite il campo `service.action.awsApiCallAction.remoteAccountDetails.accountId`.
2. Successivamente, stabilisci direttamente sul campo se quell'account è affiliato al tuo GuardDuty ambiente. `service.action.awsApiCallAction.remoteAccountDetails.affiliated`
3. Se l'account è affiliato, contatta il proprietario dell'account remoto e il proprietario delle credenziali dell'istanza EC2 per ulteriori indagini.
4. Se l'account non è affiliato, per prima cosa valuta se è associato alla tua organizzazione ma non fa parte della configurazione GuardDuty multiaccount o se non GuardDuty è ancora stato abilitato nell'account. Altrimenti contatta il proprietario delle credenziali EC2 per determinare se esiste un caso d'uso che prevede l'utilizzo di tali credenziali da parte dell'account remoto.
5. Se il proprietario non riconosce l'account remoto, allora le credenziali potrebbero essere state compromesse da un autore di minacce che opera all'interno di AWS. Segui i passaggi consigliati in Correzione di un'istanza Amazon EC2 potenzialmente compromessa per proteggere il tuo ambiente. Inoltre, puoi inviare una segnalazione di abuso al team AWS Trust and Safety per avviare un'indagine sull'account remoto. Quando invii la segnalazione a Fiducia e sicurezza di AWS , includi i dettagli JSON completi dell'esito.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Credenziali create in modo esclusivo per un'istanza EC2 mediante un ruolo di avvio di istanze vengono utilizzate da un indirizzo IP esterno.

Gravità predefinita: alta

- Fonte dei dati: eventi CloudTrail di gestione o eventi relativi ai dati S3

Questo risultato indica che un host esterno AWS ha tentato di eseguire operazioni AWS API utilizzando AWS credenziali temporanee create su un'istanza EC2 nel tuo ambiente. AWS L'istanza EC2 elencata potrebbe essere compromessa e le credenziali temporanee di questa istanza potrebbero essere state esfiltrate su un host remoto esterno a. AWS AWS non consiglia di ridistribuire le credenziali temporanee all'esterno dell'entità che le ha create (ad esempio, AWS applicazioni, EC2 o Lambda). Tuttavia, gli utenti autorizzati possono esportare le credenziali dalle proprie istanze EC2 per rendere legittime le chiamate API. Per escludere un potenziale attacco e verificare la legittimità dell'attività, verifica se nell'esito è previsto l'uso di credenziali di istanza provenienti dall'IP remoto.

> **Note**
>
> Se GuardDuty rileva un'attività continua da un account remoto, il modello di machine learning (ML) lo identificherà come un comportamento previsto. Pertanto, GuardDuty smetterà di generare questo risultato per l'attività da quell'account remoto. GuardDuty continuerà a generare risultati relativi a nuovi comportamenti provenienti da altri account remoti e rivaluterà gli account remoti appresi man mano che il comportamento cambia nel tempo.

Raccomandazioni per la correzione:

Questo esito viene generato quando la rete è configurata per instradare il traffico Internet in modo tale da uscire da un gateway on-premise anziché da un gateway Internet (IGW) VPC. Configurazioni comuni, come l'utilizzo di AWS Outposts o delle connessioni VPN del VPC, possono instradare il traffico in questo modo. Se questo comportamento è previsto, ti consigliamo di utilizzare le regole di eliminazione e creare una regola composta da due criteri di filtro. Il primo criterio è trovare il tipo, che dovrebbe essere `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. Il secondo criterio di filtro è l'Indirizzo IPv4 del chiamante API con l'indirizzo IP o l'intervallo CIDR del gateway Internet on-premise. Per ulteriori informazioni sulla creazione di regole di soppressione, vedere Regole di eliminazione.

> **Note**
>
> Se GuardDuty rileva un'attività continua da una fonte esterna, il suo modello di apprendimento automatico identificherà questa come comportamento previsto e smetterà di generare questo risultato per l'attività proveniente da quella fonte. GuardDuty continuerà a generare risultati per nuovi comportamenti da altre fonti e rivaluterà le fonti apprese man mano che il comportamento cambia nel tempo.

Se questa attività non è prevista, le credenziali potrebbero essere compromesse, vedere Riparazione delle credenziali potenzialmente compromesse AWS.

UnauthorizedAccess:IAMUser/MaliciousIPCaller

Un'API è stata chiamata da un indirizzo IP dannoso noto.

Gravità predefinita: media

- Fonte dei dati: eventi CloudTrail di gestione

Questa scoperta ti informa che un'operazione API (ad esempio, un tentativo di avviare un'istanza EC2, creare un nuovo utente IAM o modificare AWS i tuoi privilegi) è stata richiamata da un indirizzo IP malevolo noto. Ciò può indicare un accesso non autorizzato alle risorse all'interno dell'ambiente. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

Un'API è stata chiamata da un indirizzo IP incluso in un elenco di minacce personalizzato.

Gravità predefinita: media

- Fonte dei dati: eventi CloudTrail di gestione

Questa scoperta ti informa che un'operazione API (ad esempio, un tentativo di avviare un'istanza EC2, creare un nuovo utente IAM o modificare AWS i privilegi) è stata richiamata da un indirizzo IP incluso in un elenco di minacce che hai caricato. In GuardDuty, un elenco minacce include indirizzi IP dannosi noti. Ciò può indicare un accesso non autorizzato alle risorse all'interno del tuo ambiente AWS .

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

UnauthorizedAccess:IAMUser/TorIPCaller

Un'API è stata chiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: media

- Fonte dei dati: eventi CloudTrail di gestione

Questo esito segnala che un'operazione API (ad esempio, un tentativo di avviare un'istanza EC2, creare un nuovo utente IAM o modificare i privilegi AWS) è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle risorse AWS con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Tipi di esiti dei log di audit di Kubernetes

I seguenti esiti sono specifici per le risorse Kubernetes e hanno un resource_type di `EKSCluster`. La gravità e i dettagli degli esiti variano in base al tipo di esito.

Per tutti i tipi di esiti di Kubernetes, ti consigliamo di esaminare la risorsa in questione per determinare se l'attività è prevista o potenzialmente dannosa. Per indicazioni su come correggere una risorsa Kubernetes compromessa identificata da un risultato, consulta. GuardDuty Correzione degli esiti del monitoraggio dei log di audit EKS

> **Note**
>
> Se questi esiti vengono generati a causa di un'attività prevista, valuta la possibilità di aggiungere una Regole di eliminazione per evitare avvisi futuri.

Argomenti

- 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/ContainerWithSensitiveMount
- 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
- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- 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**
>
> Prima della versione 1.14 di Kubernetes, il gruppo era associato a e per impostazione predefinita. `system:unauthenticated` `system:discovery` `system:basic-user` ClusterRoles Questa associazione potrebbe consentire l'accesso non intenzionale a utenti anonimi. Gli aggiornamenti del cluster non revocano queste autorizzazioni. Anche se hai aggiornato il cluster alla versione 1.14 o successiva, le autorizzazioni in questione potrebbero essere ancora abilitate. Ti consigliamo di disassociare queste autorizzazioni dal gruppo `system:unauthenticated`. Per indicazioni sulla revoca di queste autorizzazioni, consulta le best practice di sicurezza per Amazon EKS nella Amazon EKS User Guide.

CredentialAccess:Kubernetes/MaliciousIPCaller

Un'API comunemente utilizzata per accedere a credenziali o segreti in un cluster Kubernetes è stata richiamata da un indirizzo IP dannoso noto.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'operazione API è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata alle tattiche di accesso alle credenziali in cui un avversario tenta di raccogliere password, nomi utente e chiavi di accesso per il cluster Kubernetes.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è`system:anonymous`, scopri perché all'utente anonimo è stato consentito di richiamare l'API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al

cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

Un'API comunemente utilizzata per accedere a credenziali o segreti in un cluster Kubernetes è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'operazione API è stata chiamata da un indirizzo IP incluso in un elenco minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. L'API osservata è comunemente associata alle tattiche di accesso alle credenziali in cui un avversario tenta di raccogliere password, nomi utente e chiavi di accesso per il cluster Kubernetes.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è`system:anonymous`, verifica il motivo per cui all'utente anonimo è stato consentito richiamare l'API e revoca le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

Un'API comunemente utilizzata per accedere a credenziali o segreti in un cluster Kubernetes è stata richiamata da un utente non autenticato.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'operazione API è stata richiamata correttamente dall'utente `system:anonymous`. Le chiamate API effettuate da `system:anonymous` non sono autenticate. L'API osservata è comunemente associata alle tattiche di accesso alle credenziali in cui un avversario tenta di raccogliere password, nomi utente e chiavi di accesso per il cluster Kubernetes. Questa attività indica che è stato autorizzato l'accesso anonimo o non autenticato sull'operazione API riportata nell'esito e che l'accesso potrebbe essere autorizzato anche su altre operazioni. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` sul cluster e assicurati che tutte le autorizzazioni siano necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta le best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS.

Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

CredentialAccess:Kubernetes/TorIPCaller

Un'API comunemente utilizzata per accedere a credenziali o segreti in un cluster Kubernetes è stata richiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'API è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. L'API osservata è comunemente associata alle tattiche di accesso alle credenziali in cui un avversario tenta di raccogliere password, nomi utente e chiavi di accesso per il cluster Kubernetes. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle risorse del cluster Kubernetes con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è`system:anonymous`, scopri perché all'utente anonimo è stato consentito di richiamare l'API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

DefenseEvasion:Kubernetes/MaliciousIPCaller

Un'API comunemente utilizzata per eludere le misure difensive è stata richiamata da un indirizzo IP dannoso noto.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'operazione API è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata a tattiche di evasione della difesa in cui un avversario cerca di nascondere le proprie operazioni per non essere rilevato.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è`system:anonymous`, scopri perché all'utente anonimo è stato consentito di richiamare l'API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

Un'API comunemente utilizzata per eludere le misure difensive è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'operazione API è stata chiamata da un indirizzo IP incluso in un elenco minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. L'API osservata è comunemente associata a tattiche di evasione della difesa in cui un avversario cerca di nascondere le proprie operazioni per non essere rilevato.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è`system:anonymous`, scopri perché all'utente anonimo è stato consentito di richiamare l'API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

Un'API comunemente utilizzata per eludere le misure difensive è stata richiamata da un utente non autenticato.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'operazione API è stata richiamata correttamente dall'utente `system:anonymous`. Le chiamate API effettuate da `system:anonymous` non sono autenticate. L'API osservata è comunemente associata a tattiche di evasione della difesa in cui un avversario cerca di nascondere le proprie operazioni per non essere rilevato. Questa attività indica che è stato autorizzato l'accesso anonimo o non autenticato sull'operazione API riportata nell'esito e che l'accesso potrebbe essere autorizzato anche su altre operazioni. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` sul cluster e assicurati che tutte le autorizzazioni siano necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta le best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS.

Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

DefenseEvasion:Kubernetes/TorIPCaller

Un'API comunemente utilizzata per eludere le misure difensive è stata richiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'API è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. L'API osservata è comunemente associata a tattiche di evasione della difesa in cui un avversario cerca di nascondere le proprie operazioni per non essere rilevato. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato al cluster Kubernetes con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è`system:anonymous`, scopri perché all'utente anonimo è stato consentito di richiamare l'API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Discovery:Kubernetes/MaliciousIPCaller

Un'API comunemente utilizzata per scovare risorse in un cluster Kubernetes è stata richiamata da un indirizzo IP.

Gravità predefinita: media

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'operazione API è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata alla fase di scoperta di un attacco in cui l'utente malintenzionato raccoglie informazioni per determinare se il cluster Kubernetes è suscettibile a un attacco più ampio.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è`system:anonymous`, scopri perché all'utente anonimo è stato consentito di richiamare l'API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Discovery:Kubernetes/MaliciousIPCaller.Custom

Un'API comunemente utilizzata per scovare risorse in un cluster Kubernetes è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: media

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'API è stata richiamata da un indirizzo IP incluso in un elenco minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni

aggiuntive dei dettagli di un esito. L'API osservata è comunemente associata alla fase di scoperta di un attacco in cui l'utente malintenzionato raccoglie informazioni per determinare se il cluster Kubernetes è suscettibile a un attacco più ampio.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è`system:anonymous`, scopri perché all'utente anonimo è stato consentito di richiamare l'API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Discovery:Kubernetes/SuccessfulAnonymousAccess

Un'API comunemente utilizzata per scovare risorse in un cluster Kubernetes è stata richiamata da un utente non autenticato.

Gravità predefinita: media

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'operazione API è stata richiamata correttamente dall'utente `system:anonymous`. Le chiamate API effettuate da `system:anonymous` non sono autenticate. L'API osservata è comunemente associata alla fase di scoperta di un attacco, quando un avversario raccoglie informazioni sul cluster Kubernetes. Questa attività indica che è stato autorizzato l'accesso anonimo o non autenticato sull'operazione API riportata nell'esito e che l'accesso potrebbe essere autorizzato anche su altre operazioni. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` sul cluster e assicurati che tutte le autorizzazioni siano necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata

apportata al cluster da un avversario. Per ulteriori informazioni, consulta le best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS.

Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Discovery:Kubernetes/TorIPCaller

Un'API comunemente utilizzata per scovare risorse in un cluster Kubernetes è stata richiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: media

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'API è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. L'API osservata è comunemente associata alla fase di scoperta di un attacco in cui l'utente malintenzionato raccoglie informazioni per determinare se il cluster Kubernetes è suscettibile a un attacco più ampio. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato al cluster Kubernetes con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la *`KubernetesUserDetails`* sezione lo è*`system:anonymous`*, scopri perché all'utente anonimo è stato consentito di richiamare l'API e revoca le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Execution:Kubernetes/ExecInKubeSystemPod

È stato eseguito un comando in un pod all'interno dello spazio dei nomi del **`kube-system`**.

Gravità predefinita: media

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che è stato eseguito un comando in un pod all'interno dello spazio dei nomi del `kube-system` utilizzando l'API di esecuzione Kubernetes. Lo spazio dei nomi del `kube-system` è predefinito e viene utilizzato principalmente per componenti a livello di sistema, come `kube-dns` e `kube-proxy`. L'esecuzione di comandi in pod o container all'interno dello spazio dei nomi del `kube-system` è molto rara e può indicare attività sospette.

Raccomandazioni per la correzione:

Se l'esecuzione di questo comando non è prevista, le credenziali dell'identità utente utilizzate per eseguirlo potrebbero essere compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Impact:Kubernetes/MaliciousIPCaller

Un'API comunemente utilizzata per manomettere risorse in un cluster Kubernetes è stata richiamata da un indirizzo IP dannoso noto.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'operazione API è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata a tattiche di impatto in cui un avversario tenta di manipolare, interrompere o distruggere i dati all'interno del tuo ambiente. AWS

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è`system:anonymous`, scopri perché all'utente anonimo è stato consentito di richiamare l'API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Impact:Kubernetes/MaliciousIPCaller.Custom

Un'API comunemente utilizzata per manomettere risorse in un cluster Kubernetes è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'operazione API è stata chiamata da un indirizzo IP incluso in un elenco minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. L'API osservata è comunemente associata a tattiche di impatto in cui un avversario tenta di manipolare, interrompere o distruggere i dati all'interno del tuo ambiente. AWS

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è`system:anonymous`, scopri perché all'utente anonimo è stato consentito di richiamare l'API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Impact:Kubernetes/SuccessfulAnonymousAccess

Un'API comunemente utilizzata per manomettere risorse in un cluster Kubernetes è stata richiamata da un utente non autenticato.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'operazione API è stata richiamata correttamente dall'utente `system:anonymous`. Le chiamate API effettuate da `system:anonymous` non sono autenticate.

L'API osservata è generalmente associata alla fase di impatto di un attacco, quando un avversario manomette le risorse del cluster. Questa attività indica che è stato autorizzato l'accesso anonimo o non autenticato sull'operazione API riportata nell'esito e che l'accesso potrebbe essere autorizzato anche su altre operazioni. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` sul cluster e assicurati che tutte le autorizzazioni siano necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta le best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS.

Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Impact:Kubernetes/TorIPCaller

Un'API comunemente utilizzata per manomettere risorse in un cluster Kubernetes è stata richiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'API è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. L'API osservata è comunemente associata a tattiche di impatto con cui un avversario cerca di manipolare, interrompere o distruggere dati all'interno del tuo ambiente AWS . Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato al cluster Kubernetes con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è`system:anonymous`, scopri perché all'utente anonimo è stato consentito di richiamare l'API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato,

effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Persistence:Kubernetes/ContainerWithSensitiveMount

È stato avviato un container con un percorso host esterno sensibile montato all'interno.

Gravità predefinita: media

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un container è stato avviato con una configurazione che includeva un percorso host sensibile con accesso in scrittura nella sezione `volumeMounts`. Ciò rende questo percorso accessibile e scrivibile dall'interno del container. Questa tecnica viene comunemente utilizzata dagli avversari per accedere al file system dell'host.

Raccomandazioni per la correzione:

Se l'avvio del container non è previsto, le credenziali dell'identità utente utilizzate per avviarlo potrebbero essere compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se l'avvio di questo container è previsto, ti consigliamo di utilizzare una regola di eliminazione composta da un criterio di filtro basato sul campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nei criteri di filtro, il campo `imagePrefix` deve essere uguale all'`imagePrefix` specificato nell'esito. Per ulteriori informazioni sulla creazione delle regole di eliminazione, consulta Regole di eliminazione.

Persistence:Kubernetes/MaliciousIPCaller

Un'API comunemente utilizzata per mantenere l'accesso persistente a un cluster Kubernetes è stata richiamata da un indirizzo IP dannoso noto.

Gravità predefinita: media

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'operazione API è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata a tattiche di persistenza in cui un avversario ha ottenuto l'accesso al cluster Kubernetes e cerca di mantenerlo.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è`system:anonymous`, scopri perché all'utente anonimo è stato consentito di richiamare l'API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Persistence:Kubernetes/MaliciousIPCaller.Custom

Un'API comunemente utilizzata per mantenere l'accesso persistente a un cluster Kubernetes è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: media

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'operazione API è stata chiamata da un indirizzo IP incluso in un elenco minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. L'API osservata è comunemente associata a tattiche di persistenza in cui un avversario ha ottenuto l'accesso al cluster Kubernetes e cerca di mantenerlo.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è`system:anonymous`, scopri perché all'utente anonimo è stato consentito di richiamare l'API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di

sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Persistence:Kubernetes/SuccessfulAnonymousAccess

Un'API comunemente utilizzata per ottenere autorizzazioni di alto livello per un cluster Kubernetes è stata richiamata da un utente non autenticato.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'operazione API è stata richiamata correttamente dall'utente `system:anonymous`. Le chiamate API effettuate da `system:anonymous` non sono autenticate. L'API osservata è comunemente associata alle tattiche di persistenza in cui un avversario ha ottenuto l'accesso al cluster e cerca di mantenerlo. Questa attività indica che è stato autorizzato l'accesso anonimo o non autenticato sull'operazione API riportata nell'esito e che l'accesso potrebbe essere autorizzato anche su altre operazioni. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` sul cluster e assicurati che tutte le autorizzazioni siano necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta le best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS.

Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Persistence:Kubernetes/TorIPCaller

Un'API comunemente utilizzata per mantenere l'accesso persistente a un cluster Kubernetes è stata richiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: media

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'API è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. L'API osservata è comunemente associata a tattiche di persistenza in cui un avversario ha ottenuto l'accesso al cluster Kubernetes e cerca di mantenerlo. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle tue AWS risorse con l'intento di nascondere la vera identità dell'aggressore.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è`system:anonymous`, scopri perché all'utente anonimo è stato consentito di richiamare l'API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS. Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

All'account di servizio predefinito sono stati concessi i privilegi di amministratore su un cluster Kubernetes.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che all'account di servizio predefinito per uno spazio dei nomi nel cluster Kubernetes sono stati concessi i privilegi di amministratore. Kubernetes crea un account di servizio predefinito per tutti gli spazi dei nomi del cluster e lo assegna automaticamente come identità ai pod che non sono stati associati esplicitamente a un altro account di servizio. Se l'account di servizio predefinito dispone di privilegi di amministratore, è possibile che vengano lanciati involontariamente pod con privilegi di amministratore. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Raccomandazioni per la correzione:

Non utilizzare l'account di servizio predefinito per concedere autorizzazioni ai pod. Crea invece un account di servizio dedicato per ogni carico di lavoro e concedi l'autorizzazione a tale account in base alle esigenze. Per risolvere questo problema, crea account di servizio dedicati per tutti i tuoi pod e carichi di lavoro e aggiornali per migrare dall'account di servizio predefinito ai relativi account dedicati. Rimuovi quindi l'autorizzazione di amministratore dall'account di servizio predefinito. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Policy:Kubernetes/AnonymousAccessGranted

All'utente **`system:anonymous`** è stata concessa l'autorizzazione API su un cluster Kubernetes.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un utente del cluster Kubernetes ha creato correttamente un `ClusterRoleBinding` o `RoleBinding` per associare l'utente `system:anonymous` a un ruolo. In questo modo viene consentito l'accesso non autenticato alle operazioni API autorizzate dal ruolo. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` o al gruppo `system:unauthenticated` sul cluster e revoca l'accesso anonimo non necessario. Per ulteriori informazioni, consulta le best practice di sicurezza per Amazon EKS nella Guida per l'utente di Amazon EKS. Se le autorizzazioni sono state concesse intenzionalmente, revoca l'accesso dell'utente che le ha concesse e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Policy:Kubernetes/ExposedDashboard

Il pannello di un cluster Kubernetes era esposto a Internet

Gravità predefinita: media

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che il pannello Kubernetes per il cluster è stato esposto a Internet da un servizio del sistema di bilanciamento del carico. Un pannello esposto rende l'interfaccia di gestione del cluster accessibile da Internet e consente agli avversari di sfruttare eventuali lacune nell'autenticazione e nel controllo degli accessi.

Raccomandazioni per la correzione:

Assicurati di applicare autenticazione e autorizzazione avanzate sul pannello Kubernetes. Inoltre, implementa il controllo dell'accesso alla rete per limitare l'accesso al pannello da indirizzi IP specifici.

Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Policy:Kubernetes/KubeflowDashboardExposed

Il pannello Kubeflow di un cluster Kubernetes era esposto a Internet

Gravità predefinita: media

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che il pannello Kubeflow per il cluster è stato esposto a Internet da un servizio del sistema di bilanciamento del carico. Un pannello Kubeflow esposto rende l'interfaccia di gestione dell'ambiente Kubeflow accessibile da Internet e consente agli avversari di sfruttare eventuali lacune nell'autenticazione e nel controllo degli accessi.

Raccomandazioni per la correzione:

Assicurati di applicare autenticazione e autorizzazione avanzate sul pannello Kubeflow. Inoltre, implementa il controllo dell'accesso alla rete per limitare l'accesso al pannello da indirizzi IP specifici.

Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

PrivilegeEscalation:Kubernetes/PrivilegedContainer

Un container privilegiato con accesso a livello root è stato avviato sul cluster Kubernetes.

Gravità predefinita: media

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un container privilegiato è stato avviato sul cluster Kubernetes utilizzando un'immagine che non era mai stata utilizzata per avviare container privilegiati nel cluster. Un container privilegiato ha accesso di livello root all'host. Gli avversari possono avviare container privilegiati come tattica di escalation dei privilegi per accedere all'host e quindi comprometterlo.

Raccomandazioni per la correzione:

Se l'avvio del container non è previsto, le credenziali dell'identità utente utilizzate per avviarlo potrebbero essere compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

Un'API Kubernetes comunemente utilizzata per accedere a segreti è stata richiamata in modo anomalo.

Gravità predefinita: media

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'operazione API anomala volta a recuperare segreti sensibili del cluster è stata richiamata da un utente Kubernetes del cluster. L'API osservata è comunemente associata a tattiche di accesso alle credenziali che possono portare a un'escalation dei privilegi e a ulteriori accessi all'interno del cluster. Se questo comportamento non è previsto, può indicare un errore di configurazione o che AWS le tue credenziali sono compromesse.

L'API osservata è stata identificata come anomala dal modello di machine learning (ML) per il rilevamento delle GuardDuty anomalie. Il modello di ML valuta tutte le attività delle API degli utenti all'interno del cluster EKS e identifica gli eventi anomali associati alle tecniche utilizzate da utenti non autorizzati. Il modello di ML tiene traccia di diversi fattori dell'operazione API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'agente utente utilizzato e lo spazio dei

nomi gestito dall'utente. Puoi trovare i dettagli insoliti della richiesta API nel pannello dei dettagli di ricerca della console. GuardDuty

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente Kubernetes nel cluster e assicurati che siano tutte necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se AWS le tue credenziali sono compromesse, consulta. Riparazione delle credenziali potenzialmente compromesse AWS

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

Nel cluster RoleBinding ClusterRoleBinding Kubernetes è stato creato o modificato un ruolo o un namespace riservato eccessivamente permissivo.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se un RoleBinding or ClusterRoleBinding coinvolge o, la gravità è Alta. ClusterRoles `admin` `cluster-admin`

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un utente del cluster Kubernetes ha creato un `RoleBinding` o un `ClusterRoleBinding` per associare un utente a un ruolo con autorizzazioni di amministratore o spazi dei nomi sensibili. Se questo comportamento non è previsto, può indicare un errore di configurazione o che le AWS credenziali sono compromesse.

L'API osservata è stata identificata come anomala dal modello di machine learning (ML) per il rilevamento delle GuardDuty anomalie. Il modello di ML valuta tutte le attività delle API degli utenti all'interno del cluster EKS. Questo modello di ML identifica anche gli eventi anomali associati alle

tecniche utilizzate da un utente non autorizzato. Il modello di ML tiene anche traccia di diversi fattori dell'operazione API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'agente utente utilizzato e lo spazio dei nomi gestito dall'utente. Puoi trovare i dettagli insoliti della richiesta API nel pannello dei dettagli di ricerca della console. GuardDuty

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente Kubernetes. Queste autorizzazioni sono definite nel ruolo e nei soggetti coinvolti nel `RoleBinding` e nel `ClusterRoleBinding`. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se AWS le tue credenziali sono compromesse, consulta. Riparazione delle credenziali potenzialmente compromesse AWS

Execution:Kubernetes/AnomalousBehavior.ExecInPod

È stato eseguito un comando in un pod in modo anomalo.

Gravità predefinita: media

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un comando è stato eseguito in un pod utilizzando l'API di esecuzione Kubernetes. L'API di esecuzione Kubernetes consente di eseguire di comandi arbitrari in un pod. Se questo comportamento non è previsto per l'utente, lo spazio dei nomi o il pod, può indicare un errore di configurazione o che le AWS credenziali sono compromesse.

L'API osservata è stata identificata come anomala dal modello di apprendimento automatico per il rilevamento delle GuardDuty anomalie (ML). Il modello di ML valuta tutte le attività delle API degli utenti all'interno del cluster EKS. Questo modello di ML identifica anche gli eventi anomali associati alle tecniche utilizzate da un utente non autorizzato. Il modello di ML tiene anche traccia di diversi fattori dell'operazione API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'agente utente utilizzato e lo spazio dei nomi gestito dall'utente. Puoi trovare i dettagli insoliti della richiesta API nel pannello dei dettagli di ricerca della console. GuardDuty

Raccomandazioni per la correzione:

Se l'esecuzione di questo comando non è prevista, le credenziali dell'identità utente utilizzate per eseguirlo potrebbero essere state compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se AWS le tue credenziali sono compromesse, consulta. Riparazione delle credenziali potenzialmente compromesse AWS

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

Un carico di lavoro è stato avviato in modo anomalo con un container privilegiato.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che è stato avviato un carico di lavoro con un container privilegiato nel cluster Amazon EKS. Un container privilegiato ha accesso di livello root all'host. Gli utenti non autorizzati possono avviare container privilegiati come tattica di escalation dei privilegi prima per accedere all'host, poi per comprometterlo.

La creazione o la modifica del contenitore osservata è stata identificata come anomala dal modello di apprendimento automatico per il rilevamento delle GuardDuty anomalie (ML). Il modello di ML valuta tutte le attività degli utenti legate all'API e all'immagine del container all'interno del cluster EKS. Questo modello di ML identifica anche gli eventi anomali associati alle tecniche utilizzate da un utente non autorizzato. Il modello di ML tiene anche traccia di diversi fattori dell'operazione API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'agente utente utilizzato, le immagini del container osservate nell'account e lo spazio dei nomi gestito dall'utente. Puoi trovare i dettagli insoliti della richiesta API nel pannello dei dettagli di ricerca della console. GuardDuty

Raccomandazioni per la correzione:

Se l'avvio del container non è previsto, le credenziali dell'identità utente utilizzate per avviarlo potrebbero essere state compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se AWS le tue credenziali sono compromesse, consulta. Riparazione delle credenziali potenzialmente compromesse AWS

Se l'avvio di questo container è previsto, ti consigliamo di utilizzare una regola di eliminazione con un criterio di filtro basato sul campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nei criteri di filtro, il campo `imagePrefix` deve avere lo stesso valore del campo `imagePrefix` specificato nell'esito. Per ulteriori informazioni, consulta Regole di eliminazione.

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed! ContainerWithSensitiveMount

Un carico di lavoro è stato implementato in modo anomalo con un percorso host sensibile montato al suo interno.

Gravità predefinita: alta

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un carico di lavoro è stato avviato con un container che includeva un percorso host sensibile nella sezione `volumeMounts`. Ciò rende questo percorso potenzialmente accessibile e scrivibile dall'interno del container. Questa tecnica viene comunemente utilizzata dagli utenti non autorizzati per accedere al file system dell'host.

La creazione o la modifica del contenitore osservata è stata identificata come anomala dal modello di apprendimento automatico per il rilevamento delle GuardDuty anomalie (ML). Il modello di ML valuta tutte le attività degli utenti legate all'API e all'immagine del container all'interno del cluster EKS. Questo modello di ML identifica anche gli eventi anomali associati alle tecniche utilizzate da un utente non autorizzato. Il modello di ML tiene anche traccia di diversi fattori dell'operazione API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'agente utente utilizzato, le immagini del container osservate nell'account e lo spazio dei nomi gestito dall'utente. Puoi trovare i dettagli insoliti della richiesta API nel pannello dei dettagli di ricerca della console. GuardDuty

Raccomandazioni per la correzione:

Se l'avvio del container non è previsto, le credenziali dell'identità utente utilizzate per avviarlo potrebbero essere state compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale

modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se AWS le tue credenziali sono compromesse, consulta. Riparazione delle credenziali potenzialmente compromesse AWS

Se l'avvio di questo container è previsto, ti consigliamo di utilizzare una regola di eliminazione con un criterio di filtro basato sul campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nei criteri di filtro, il campo `imagePrefix` deve avere lo stesso valore del campo `imagePrefix` specificato nell'esito. Per ulteriori informazioni, consulta Regole di eliminazione.

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

Un carico di lavoro è stato avviato in modo anomalo.

Gravità predefinita: bassa*

> **Note**
>
> La gravità predefinita è bassa. Tuttavia, se il carico di lavoro contiene un nome immagine potenzialmente sospetto, ad esempio uno strumento di test di penetrazione (pen-test) noto, o un container che esegue un comando potenzialmente sospetto all'avvio, come i comandi di shell (interprete di comandi) inversa, questo tipo di esito verrà considerato di gravità media.

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un carico di lavoro Kubernetes, ad esempio un'attività API, nuove immagini del container o una configurazione rischiosa del carico di lavoro, è stato creato o modificato in modo anomalo all'interno del cluster Amazon EKS. Gli utenti non autorizzati possono avviare container come tattica per eseguire un codice arbitrario prima per accedere all'host, poi per comprometterlo.

La creazione o la modifica del contenitore osservata è stata identificata come anomala dal modello di apprendimento automatico per il rilevamento delle GuardDuty anomalie (ML). Il modello di ML valuta tutte le attività degli utenti legate all'API e all'immagine del container all'interno del cluster EKS. Questo modello di ML identifica anche gli eventi anomali associati alle tecniche utilizzate da un utente non autorizzato. Il modello di ML tiene anche traccia di diversi fattori dell'operazione API, come

l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'agente utente utilizzato, le immagini del container osservate nell'account e lo spazio dei nomi gestito dall'utente. Puoi trovare i dettagli insoliti della richiesta API nel pannello dei dettagli di ricerca della console. GuardDuty

Raccomandazioni per la correzione:

Se l'avvio del container non è previsto, le credenziali dell'identità utente utilizzate per avviarlo potrebbero essere state compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se AWS le tue credenziali sono compromesse, consulta. Riparazione delle credenziali potenzialmente compromesse AWS

Se l'avvio di questo container è previsto, ti consigliamo di utilizzare una regola di eliminazione con un criterio di filtro basato sul campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nei criteri di filtro, il campo `imagePrefix` deve avere lo stesso valore del campo `imagePrefix` specificato nell'esito. Per ulteriori informazioni, consulta Regole di eliminazione.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Un ruolo altamente permissivo o ClusterRole è stato creato o modificato in modo anomalo.

Gravità predefinita: bassa

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un'operazione API anomala volta a creare un `Role` o un `ClusterRole` con autorizzazioni eccessive è stata chiamata da un utente Kubernetes del cluster Amazon EKS. Gli attori possono utilizzare la creazione di ruoli con autorizzazioni avanzate per non utilizzare ruoli incorporati simili a quelli di amministratore ed evitare il rilevamento. Le autorizzazioni eccessive possono portare a un'escalation dei privilegi, all'esecuzione di codice in modalità remota e al potenziale controllo di uno spazio dei nomi o di un cluster. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

L'API osservata è stata identificata come anomala dal modello di machine learning (ML) per il rilevamento delle GuardDuty anomalie. Il modello di ML valuta tutte le attività delle API degli utenti

all'interno del cluster Amazon EKS e identifica gli eventi anomali associati alle tecniche utilizzate da utenti non autorizzati. Il modello di ML tiene anche traccia di diversi fattori dell'operazione API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'agente utente utilizzato, le immagini del container osservate nell'account e lo spazio dei nomi gestito dall'utente. Puoi trovare i dettagli insoliti della richiesta API nel pannello dei dettagli di ricerca della console. GuardDuty

Raccomandazioni per la correzione:

Esamina le autorizzazioni definite in `Role` o `ClusterRole` per assicurarti che tutte le autorizzazioni siano necessarie e segui i principi del privilegio minimo. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se AWS le tue credenziali sono compromesse, consulta. Riparazione delle credenziali potenzialmente compromesse AWS

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Un utente ha verificato la propria autorizzazione di accesso in modo anomalo.

Gravità predefinita: bassa

- Funzionalità: log di audit di Kubernetes

Questo esito segnala che un utente del cluster Kubernetes ha verificato correttamente se sono consentite o meno le autorizzazioni avanzate note che possono portare a un'escalation dei privilegi e all'esecuzione di codice in modalità remota. Ad esempio, `kubectl auth can-i` è un comando comune utilizzato per verificare le autorizzazioni di un utente. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono state compromesse.

L'API osservata è stata identificata come anomala dal modello di machine learning (ML) per il rilevamento delle GuardDuty anomalie. Il modello di ML valuta tutte le attività delle API degli utenti all'interno del cluster Amazon EKS e identifica gli eventi anomali associati alle tecniche utilizzate da utenti non autorizzati. Il modello di ML tiene anche traccia di diversi fattori dell'operazione API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'autorizzazione oggetto della verifica e lo spazio dei nomi gestito dall'utente. Puoi trovare i dettagli insoliti della richiesta API nel pannello dei dettagli di ricerca della console. GuardDuty

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente Kubernetes per assicurarti che siano tutte necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se AWS le tue credenziali sono compromesse, consulta. Riparazione delle credenziali potenzialmente compromesse AWS

Tipi di esiti della Protezione Lambda

Questa sezione descrive i tipi di esiti specifici delle tue risorse AWS Lambda e per i quali il `resourceType` è elencato come `Lambda`. Per tutti gli esiti di Lambda, ti consigliamo di esaminare la risorsa in questione e determinare se si comporta nel modo previsto. Se l'attività è autorizzata, puoi utilizzare le Regole di eliminazione o gli Elenchi di indirizzi IP affidabili e gli elenchi minacce per prevenire notifiche false positive per quella risorsa.

Se l'attività non è prevista, la best practice di sicurezza consiste nel presupporre che Lambda sia stata potenzialmente compromessa e seguire le raccomandazioni per la correzione.

Argomenti

- 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

Una funzione Lambda esegue una query su un indirizzo IP associato a un server di comando e controllo noto.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di rete Lambda

Questo esito segnala che la funzione Lambda elencata all'interno del tuo ambiente AWS esegue una query su un indirizzo IP associato a un server di comando e controllo (C&C) noto. La funzione Lambda associata all'esito generato è potenzialmente compromessa. I server C&C sono computer che inviano comandi ai membri di una botnet.

Una botnet è una raccolta di dispositivi connessi a Internet, come PC, server, dispositivi mobili e dispositivi Internet of Things, infettata e controllata da un tipo comune di malware. Le botnet sono spesso utilizzate per distribuire malware e rubare informazioni sensibili, ad esempio i numeri di carte di credito. A seconda dello scopo e della struttura della botnet, il server C&C potrebbe anche inviare comandi per lanciare un Distributed Denial of Service.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di una funzione Lambda potenzialmente compromessa.

CryptoCurrency:Lambda/BitcoinTool.B

Una funzione Lambda esegue una query su un indirizzo IP associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di rete Lambda

Questo esito segnala che la funzione Lambda elencata nel tuo ambiente AWS esegue una query su un indirizzo IP associato a un'attività correlata a Bitcoin o a un'altra criptovaluta. Gli autori delle minacce potrebbero cercare di assumere il controllo delle funzioni Lambda per riutilizzarle in modo dannoso per il mining non autorizzato di criptovalute.

Raccomandazioni per la correzione:

Se usi questa funzione Lambda per estrarre o gestire criptovaluta o se questa funzione è altrimenti coinvolta in un'attività di blockchain, può trattarsi di un'attività potenzialmente prevista per il tuo

ambiente. Se questo è il caso del tuo ambiente AWS, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di eliminazione deve essere costituita da due criteri di filtro. Il primo criterio deve utilizzare l'attributo tipo di esito con un valore di CryptoCurrency:Lambda/BitcoinTool.B. Il secondo criterio di filtro deve essere il nome della funzione Lambda coinvolta nell'attività di blockchain. Per informazioni sulla creazione di regole di eliminazione, consulta Regole di eliminazione.

Se questa attività non è prevista, la funzione Lambda è potenzialmente compromessa. Per ulteriori informazioni, consulta Correzione di una funzione Lambda potenzialmente compromessa.

Trojan:Lambda/BlackholeTraffic

Una funzione Lambda tenta di comunicare con l'indirizzo IP di un host remoto che è un noto buco nero.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di rete Lambda

Questo esito segnala che una funzione Lambda elencata nel tuo ambiente AWS tenta di comunicare con l'indirizzo IP di un buco nero (o sinkhole). I buchi neri sono zone della rete dove il traffico in entrata e in uscita viene eliminato silenziosamente senza che l'origine venga informata del mancato recapito dei dati al destinatario. L'indirizzo IP di un buco nero designa un computer host non in esecuzione o un indirizzo a cui non è stato assegnato alcun host. La funzione Lambda elencata è potenzialmente compromessa.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di una funzione Lambda potenzialmente compromessa.

Trojan:Lambda/DropPoint

Una funzione Lambda tenta di comunicare con l'indirizzo IP di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di rete Lambda

Questo esito segnala che una funzione Lambda elencata nel tuo ambiente AWS tenta di comunicare con l'indirizzo IP di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di una funzione Lambda potenzialmente compromessa.

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Una funzione Lambda stabilisce connessioni a un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di rete Lambda

Questo esito segnala che una funzione Lambda nel tuo ambiente AWS comunica con un indirizzo IP incluso in un elenco minacce che hai caricato. In GuardDuty, un elenco minacce include indirizzi IP dannosi noti. GuardDuty genera esiti in base agli elenchi minacce caricati. Puoi visualizzare i dettagli dell'elenco minacce nei dettagli degli esiti sulla console GuardDuty.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di una funzione Lambda potenzialmente compromessa.

UnauthorizedAccess:Lambda/TorClient

Una funzione Lambda stabilisce connessioni a un Tor Guard o a un nodo Authority.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di rete Lambda

Questo esito segnala che una funzione Lambda nel tuo ambiente AWS stabilisce connessioni a un Tor Guard o a un nodo Authority. Tor è un software che consente la comunicazione anonima. I Tor Guard e i nodi Authority fungono da gateway iniziali per una rete Tor. Questo traffico può indicare che la funzione Lambda è stata potenzialmente compromessa e al momento funge da client su una rete Tor.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di una funzione Lambda potenzialmente compromessa.

UnauthorizedAccess:Lambda/TorRelay

Una funzione Lambda stabilisce connessioni a una rete Tor come relè Tor.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di rete Lambda

Questo esito segnala che una funzione Lambda nel tuo ambiente AWS stabilisce connessioni a una rete Tor in un modo che suggerisce che funga da relè Tor. Tor è un software che consente la comunicazione anonima. Tor aumenta consente l'anonimato della comunicazione inoltrando il traffico potenzialmente illecito del client da un relè Tor a un altro.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di una funzione Lambda potenzialmente compromessa.

Tipi di esiti della protezione da malware

La protezione da malware di GuardDuty fornisce un unico esito per tutte le minacce rilevate durante la scansione di un'istanza EC2 o del carico di lavoro di un container. L'esito include il numero totale di rilevamenti effettuati durante la scansione e, in base alla gravità, fornisce dettagli sulle 32 minacce rilevate principali. A differenza di altri esiti di GuardDuty, quelli della protezione da malware non vengono aggiornati quando la stessa istanza EC2 o lo stesso carico di lavoro dello stesso container vengono nuovamente scansionati.

La protezione da malware genera un nuovo esito per ogni scansione che rileva malware. Gli esiti della protezione da malware includono informazioni sulla scansione che ha prodotto l'esito e sull'esito di GuardDuty che ha l'ha avviata. In questo modo, la correlazione tra il comportamento sospetto e il malware rilevato è più semplice.

> **Note**
>
> Quando GuardDuty rileva attività dannose sul carico di lavoro di un container, la protezione da malware non genera alcun esito a livello EC2.

Gli esiti seguenti sono specifici per la protezione da malware di GuardDuty.

Argomenti

- 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

È stato rilevato un file dannoso su un'istanza EC2.

Gravità predefinita: varia a seconda della minaccia rilevata.

Questo esito indica che la scansione della protezione da malware di GuardDuty ha rilevato uno o più file dannosi sull'istanza EC2 elencata all'interno del tuo ambiente AWS. Questa istanza elencata potrebbe essere compromessa. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Execution:ECS/MaliciousFile

È stato rilevato un file dannoso su un cluster ECS.

Gravità predefinita: varia a seconda della minaccia rilevata.

Questo esito indica che la scansione della protezione da malware di GuardDuty ha rilevato uno o più file dannosi sul carico di lavoro di un container appartenente a un cluster ECS. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il container appartenente al cluster ECS potrebbe essere compromesso. Per ulteriori informazioni, consulta Riparazione di un cluster ECS potenzialmente compromesso.

Execution:Kubernetes/MaliciousFile

È stato rilevato un file dannoso su un cluster Kubernetes.

Gravità predefinita: varia a seconda della minaccia rilevata.

Questo esito indica che la scansione della protezione da malware di GuardDuty ha rilevato uno o più file dannosi sul carico di lavoro di un container appartenente a un cluster Kubernetes. Se questo cluster è gestito da EKS, i dettagli degli esiti forniranno informazioni aggiuntive sulla risorsa EKS interessata. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il carico di lavoro del container potrebbe essere compromesso. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Execution:Container/MaliciousFile

È stato rilevato un file dannoso in un container autonomo.

Gravità predefinita: varia a seconda della minaccia rilevata.

Questo esito indica che la scansione della protezione da malware di GuardDuty ha rilevato uno o più file dannosi sul carico di lavoro di un container e non è stata identificata alcuna informazione relativa al cluster. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il carico di lavoro del container potrebbe essere compromesso. Per ulteriori informazioni, consulta Riparazione di un contenitore autonomo potenzialmente compromesso.

Execution:EC2/SuspiciousFile

È stato rilevato un file sospetto su un'istanza EC2.

Gravità predefinita: varia a seconda della minaccia rilevata.

Questo esito indica che la scansione della protezione da malware di GuardDuty ha rilevato uno o più file sospetti su un'istanza EC2. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

I rilevamenti di tipo `SuspiciousFile` indicano che su una risorsa interessata sono presenti programmi potenzialmente indesiderati come adware, spyware o strumenti a duplice uso. Questi programmi potrebbero avere un impatto negativo sulla risorsa o essere utilizzati da utenti malintenzionati per scopi dannosi. Ad esempio, gli strumenti di rete possono essere utilizzati in modo legittimo o in modo dannoso dagli avversari come strumenti di hacking per cercare di compromettere le risorse.

Quando viene rilevato un file sospetto, valuta se si tratta di un file previsto per il tuo ambiente AWS. Se il file non è previsto, segui la procedura descritta nella sezione successiva.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Execution:ECS/SuspiciousFile

È stato rilevato un file sospetto su un cluster ECS.

Gravità predefinita: varia a seconda della minaccia rilevata.

Questo esito indica che la scansione della protezione da malware di GuardDuty ha rilevato uno o più file sospetti su un container appartenente a un cluster ECS. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

I rilevamenti di tipo `SuspiciousFile` indicano che su una risorsa interessata sono presenti programmi potenzialmente indesiderati come adware, spyware o strumenti a duplice uso. Questi programmi potrebbero avere un impatto negativo sulla risorsa o essere utilizzati da utenti malintenzionati per scopi dannosi. Ad esempio, gli strumenti di rete possono essere utilizzati in modo legittimo o in modo dannoso dagli avversari come strumenti di hacking per cercare di compromettere le risorse.

Quando viene rilevato un file sospetto, valuta se si tratta di un file previsto per il tuo ambiente AWS. Se il file non è previsto, segui la procedura descritta nella sezione successiva.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il container appartenente al cluster ECS potrebbe essere compromesso. Per ulteriori informazioni, consulta Riparazione di un cluster ECS potenzialmente compromesso.

Execution:Kubernetes/SuspiciousFile

È stato rilevato un file sospetto su un cluster Kubernetes.

Gravità predefinita: varia a seconda della minaccia rilevata.

Questo esito indica che la scansione della protezione da malware di GuardDuty ha rilevato uno o più file sospetti su un container appartenente a un cluster Kubernetes. Se questo cluster è gestito da EKS, i dettagli degli esiti forniranno informazioni aggiuntive sull'EKS interessato. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

I rilevamenti di tipo `SuspiciousFile` indicano che su una risorsa interessata sono presenti programmi potenzialmente indesiderati come adware, spyware o strumenti a duplice uso. Questi programmi potrebbero avere un impatto negativo sulla risorsa o essere utilizzati da utenti malintenzionati per scopi dannosi. Ad esempio, gli strumenti di rete possono essere utilizzati in modo legittimo o in modo dannoso dagli avversari come strumenti di hacking per cercare di compromettere le risorse.

Quando viene rilevato un file sospetto, valuta se si tratta di un file previsto per il tuo ambiente AWS. Se il file non è previsto, segui la procedura descritta nella sezione successiva.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il carico di lavoro del container potrebbe essere compromesso. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Execution:Container/SuspiciousFile

È stato rilevato un file sospetto in un container autonomo.

Gravità predefinita: varia a seconda della minaccia rilevata.

Questo esito indica che la scansione della protezione da malware di GuardDuty ha rilevato uno o più file sospetti su un container senza alcuna informazione relativa al cluster. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

I rilevamenti di tipo `SuspiciousFile` indicano che su una risorsa interessata sono presenti programmi potenzialmente indesiderati come adware, spyware o strumenti a duplice uso. Questi programmi potrebbero avere un impatto negativo sulla risorsa o essere utilizzati da utenti malintenzionati per scopi dannosi. Ad esempio, gli strumenti di rete possono essere utilizzati in modo legittimo o in modo dannoso dagli avversari come strumenti di hacking per cercare di compromettere le risorse.

Quando viene rilevato un file sospetto, valuta se si tratta di un file previsto per il tuo ambiente AWS. Se il file non è previsto, segui la procedura descritta nella sezione successiva.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il carico di lavoro del container potrebbe essere compromesso. Per ulteriori informazioni, consulta Riparazione di un contenitore autonomo potenzialmente compromesso.

Tipi di esiti della Protezione RDS di GuardDuty

La Protezione RDS di GuardDuty rileva eventuali comportamenti di accesso anomali sull'istanza di database. Gli esiti seguenti sono specifici per il Database Amazon Aurora supportati e avranno un Tipo di risorsa di `RDSDBInstance`. La gravità e i dettagli dei risultati saranno diversi in base al tipo di risultato.

Argomenti

- 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

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

Un utente ha effettuato correttamente l'accesso a un database RDS del tuo account in modo anomalo.

Gravità predefinita: variabile

> **Note**
>
> A seconda del comportamento anomalo associato a questo esito, la gravità predefinita può essere bassa, media e alta.
>
> - Bassa: se il nome utente associato a questo esito ha effettuato l'accesso da un indirizzo IP associato a una rete privata.
> - Media: se il nome utente associato a questo esito ha effettuato l'accesso da un indirizzo IP pubblico.
> - Alta: se viene individuata una serie di tentativi di accesso falliti da indirizzi IP pubblici, indicativo di policy di accesso troppo permissive.

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che è stato osservato un accesso anomalo riuscito a un database RDS nel tuo ambiente AWS. Ciò può indicare che un utente che non era mai stato rilevato in precedenza ha effettuato l'accesso a un database RDS per la prima volta. Uno scenario comune consiste nell'accesso da parte di un utente interno a un database a cui accedono le applicazioni a livello di programmazione, ma non i singoli utenti.

Questo accesso riuscito è stato identificato come anomalo dal modello di machine learning (ML) di GuardDuty per il rilevamento delle anomalie. Il modello di ML valuta tutti gli eventi di accesso al database nel tuo Database Amazon Aurora supportati e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori dell'attività di accesso RDS, ad esempio l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e i dettagli specifici di connessione al database utilizzati. Per informazioni sugli eventi di accesso potenzialmente insoliti, consulta Anomalie basate sull'attività di accesso RDS.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, ti consigliamo di modificare la password dell'utente del database e di esaminare i log di audit disponibili per le attività eseguite dall'utente anomalo. Gli esiti di gravità media e alta possono indicare che la policy di accesso al database è troppo permissiva e che le credenziali dell'utente potrebbero essere state esposte o compromesse. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti.

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Uno o più tentativi di accesso insoliti falliti sono stati osservati su un database RDS del tuo account.

Gravità predefinita: bassa

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che sono stati osservati uno o più accessi anomali falliti su un database RDS nel tuo ambiente AWS. Un tentativo di accesso fallito da indirizzi IP pubblici può indicare che il database RDS del tuo account è stato oggetto di un tentativo di attacco di forza bruta da parte di un utente potenzialmente malintenzionato.

Questi accessi falliti sono stati identificati come anomali dal modello di machine learning (ML) di GuardDuty per il rilevamento delle anomalie. Il modello di ML valuta tutti gli eventi di accesso al database nel tuo Database Amazon Aurora supportati e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori dell'attività di accesso RDS, ad esempio l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e i dettagli specifici di connessione al database utilizzati. Per informazioni sulle attività di accesso RDS potenzialmente insolite, consulta Anomalie basate sull'attività di accesso RDS.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che il database è esposto pubblicamente o che la policy di accesso al database è troppo permissiva. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti.

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

Un utente ha effettuato correttamente l'accesso a un database RDS del tuo account da un indirizzo IP pubblico in modo anomalo dopo una serie di tentativi di accesso insoliti falliti.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che su un database RDS nel tuo ambiente AWS è stato osservato un accesso anomalo indicativo di un attacco di forza bruta riuscito. Prima di un accesso anomalo riuscito, è stata osservata una serie di tentativi di accesso insoliti falliti. Ciò indica che l'utente e la password associati al database RDS del tuo account potrebbero essere stati compromessi e che un utente potenzialmente malintenzionato potrebbe aver effettuato l'accesso al database RDS.

Questo accesso di forza bruta riuscito è stato identificato come anomalo dal modello di machine learning (ML) di GuardDuty per il rilevamento delle anomalie. Il modello di ML valuta tutti gli eventi di accesso al database nel tuo Database Amazon Aurora supportati e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori dell'attività di accesso RDS, ad esempio l'utente che ha effettuato la richiesta, la posizione da cui è stata

effettuata la richiesta e i dettagli specifici di connessione al database utilizzati. Per informazioni sulle attività di accesso RDS potenzialmente insolite, consulta Anomalie basate sull'attività di accesso RDS.

Raccomandazioni per la correzione:

Questa attività indica che le credenziali del database potrebbero essere state esposte o compromesse. Ti consigliamo di modificare la password dell'utente del database associato e di esaminare i log di audit disponibili per le attività eseguite dall'utente potenzialmente compromesso. Una serie di tentativi di accesso insoliti falliti indica che la policy di accesso al database è troppo permissiva o che il database potrebbe essere stato esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti.

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

Un utente ha effettuato correttamente l'accesso a un database RDS del tuo account da un indirizzo IP dannoso noto.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che si è verificata un'attività di accesso RDS riuscita a partire da un indirizzo IP associato a un'attività dannosa nota nel tuo ambiente AWS. Ciò indica che l'utente e la password associati al database RDS del tuo account potrebbero essere stati compromessi e che un utente potenzialmente malintenzionato potrebbe aver effettuato l'accesso al database RDS.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che le credenziali dell'utente sono state esposte o compromesse. Ti consigliamo di modificare la password dell'utente del database associato e di esaminare i log di audit disponibili per le attività eseguite dall'utente compromesso. Questa attività può anche indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle

origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti.

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

Un indirizzo IP associato a un'attività dannosa nota ha tentato di accedere a un database RDS del tuo account, senza riuscirci.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che un indirizzo IP associato ad attività dannose note ha tentato di accedere a un database RDS nel tuo ambiente AWS, ma non è riuscito a fornire il nome utente o la password corretti. Ciò indica che un utente potenzialmente malintenzionato potrebbe tentare di compromettere il database RDS del tuo account.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti.

Discovery:RDS/MaliciousIPCaller

Un database RDS del tuo account è stato sottoposto a probing da un indirizzo IP associato a un'attività dannosa nota, ma non è stato effettuato alcun tentativo di autenticazione.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che un database RDS nel tuo ambiente AWS è stato sottoposto a probing da un indirizzo IP associato a un'attività dannosa nota, anche se non è stato effettuato alcun

tentativo di accesso. Ciò può indicare che un utente potenzialmente malintenzionato è alla ricerca di un'infrastruttura accessibile pubblicamente.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti.

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

Un utente ha effettuato correttamente l'accesso a un database RDS del tuo account dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che un utente ha effettuato correttamente l'accesso a un database RDS nel tuo ambiente AWS dall'indirizzo IP di un nodo di uscita Tor. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relè tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle risorse RDS del tuo account con l'intento di nascondere la vera identità dell'utente anonimo.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che le credenziali dell'utente sono state esposte o compromesse. Ti consigliamo di modificare la password dell'utente del database associato e di esaminare i log di audit disponibili per le attività eseguite dall'utente compromesso. Questa attività può anche indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti.

CredentialAccess:RDS/TorIPCaller.FailedLogin

Un indirizzo IP Tor ha tentato di accedere a un database RDS del tuo account, senza riuscirci.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che l'indirizzo IP di un nodo di uscita Tor ha tentato di accedere a un database RDS nel tuo ambiente AWS, ma non è riuscito a fornire il nome utente o la password corretti. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relè tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle risorse RDS del tuo account con l'intento di nascondere la vera identità dell'utente anonimo.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti.

Discovery:RDS/TorIPCaller

Un database RDS del tuo account è stato sottoposto a probing dall'indirizzo IP di un nodo di uscita Tor, ma non è stato effettuato alcun tentativo di autenticazione.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che un database RDS nel tuo ambiente AWS è stato sottoposto a probing dall'indirizzo IP di un nodo di uscita Tor, anche se non è stato effettuato alcun tentativo di accesso. Ciò può indicare che un utente potenzialmente malintenzionato è alla ricerca di infrastrutture

accessibili pubblicamente. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relè tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle risorse RDS del tuo account con l'intento di nascondere la vera identità dell'utente potenzialmente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti.

Tipi di risultati del monitoraggio del runtime

Amazon GuardDuty genera i seguenti risultati di Runtime Monitoring per indicare potenziali minacce in base al comportamento a livello di sistema operativo degli host e contenitori Amazon EC2 nei cluster Amazon EKS, nei carichi di lavoro Fargate e Amazon ECS e nelle istanze Amazon EC2.

> **Note**
>
> I tipi di esiti del monitoraggio del runtime EKS si basano sui log di runtime raccolti dagli host. I log contengono campi, come i percorsi dei file, che potrebbero essere controllati da un utente malintenzionato. Questi campi sono inclusi anche nei risultati per fornire un contesto di runtime. GuardDuty Quando si elaborano i risultati del Runtime Monitoring all'esterno della GuardDuty console, è necessario ripulire i campi di ricerca. Ad esempio, puoi codificare in HTML i campi degli esiti quando li visualizzi su una pagina Web.

Argomenti

- 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

CryptoCurrency:Runtime/BitcoinTool.B

Un'istanza Amazon EC2 o un container eseguono una query su un indirizzo IP associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo esito segnala che l'istanza EC2 elencata o un container nel tuo ambiente AWS eseguono una query su un indirizzo IP associato a un'attività correlata a una criptovaluta. Gli autori delle minacce potrebbero cercare di assumere il controllo delle risorse di calcolo per riutilizzarle in modo dannoso per il mining non autorizzato di criptovalute.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se utilizzi questa istanza EC2 o un container per estrarre o gestire criptovaluta o se questi elementi sono altrimenti coinvolti nell'attività di blockchain, l'esito CryptoCurrency:Runtime/BitcoinTool.B potrebbe rappresentare un'attività prevista per il tuo ambiente. Se questo è il caso nel tuo AWS ambiente, ti consigliamo di impostare una regola di soppressione per questo risultato. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio di filtro deve utilizzare l'attributo Tipo di risultato con un valore di `CryptoCurrency:Runtime/BitcoinTool.B`. Il secondo criterio di filtro deve essere l'ID istanza dell'istanza o l'ID immagine del container del container coinvolti in attività legate alle criptovalute o alla blockchain. Per ulteriori informazioni, consulta Regole di eliminazione.

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Backdoor:Runtime/C&CActivity.B

Un'istanza Amazon EC2 o un container eseguono una query su un IP associato a un server di comando e controllo noto.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo esito segnala che l'istanza EC2 elencata o un container all'interno del tuo ambiente AWS eseguono una query su un IP associato a un server di comando e controllo (C&C) noto. L'istanza elencata o il container potrebbero essere potenzialmente compromessi. I server di comando e controllo sono computer che inviano comandi ai membri di una botnet.

Una botnet è una raccolta di dispositivi connessi a Internet, come PC, server, dispositivi mobili e dispositivi Internet of Things, che sono infettati e controllati da un tipo comune di malware. Le botnet sono spesso utilizzate per distribuire malware e rubare informazioni sensibili, ad esempio i numeri di carte di credito. A seconda dello scopo e della struttura della botnet, il server C&C potrebbe anche inviare comandi per lanciare un attacco DDoS (Distributed Denial of Service).

> **Note**
>
> Se l'IP su cui viene eseguita una query è correlato a log4j, i campi dell'esito associato includeranno i valori seguenti:
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

UnauthorizedAccess:Runtime/TorRelay

L'istanza Amazon EC2 o un container stabiliscono connessioni a una rete Tor come relè Tor.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che un'istanza EC2 o un contenitore nel tuo AWS ambiente sta effettuando connessioni a una rete Tor in un modo che suggerisce che stia agendo come un relè Tor. Tor è un software che consente la comunicazione anonima. Tor aumenta l'anonimato della comunicazione inoltrando il traffico potenzialmente illecito del client da un relè Tor a un altro.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

UnauthorizedAccess:Runtime/TorClient

L'istanza Amazon EC2 o un container stabiliscono connessioni a un Tor Guard o a un nodo Authority.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che un'istanza EC2 o un contenitore nel tuo AWS ambiente sta effettuando connessioni a un nodo Tor Guard o a un nodo Authority. Tor è un software che consente la comunicazione anonima. I Tor Guard e i nodi fungono da gateway iniziali per una rete Tor. Questo traffico può indicare che l'istanza EC2 o il container sono stati compromessi e fungono da client su una rete Tor. Questa scoperta potrebbe indicare un accesso non autorizzato alle tue AWS risorse con l'intento di nascondere la vera identità dell'aggressore.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della console. GuardDuty

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Trojan:Runtime/BlackholeTraffic

Un'istanza Amazon EC2 o un container tentano di comunicare con l'indirizzo IP di un host remoto che è un noto buco nero.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questa scoperta indica che l'istanza EC2 elencata o un contenitore nel tuo AWS ambiente potrebbe essere compromesso perché sta tentando di comunicare con l'indirizzo IP di un buco nero (o sink hole). I buchi neri sono zone della rete dove il traffico in entrata e in uscita viene eliminato silenziosamente senza che l'origine venga informata del mancato recapito dei dati al destinatario. L'indirizzo IP di un buco nero designa un computer host non in esecuzione o un indirizzo a cui non è stato assegnato alcun host.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Trojan:Runtime/DropPoint

Un'istanza Amazon EC2 o un container tentano di comunicare con l'indirizzo IP di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questa scoperta indica che un'istanza EC2 o un contenitore nel tuo AWS ambiente sta tentando di comunicare con un indirizzo IP di un host remoto noto per contenere credenziali e altri dati rubati acquisiti da malware.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

CryptoCurrency:Runtime/BitcoinTool.B!DNS

Un'istanza Amazon EC2 o un container eseguono una query su un nome di dominio associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo esito segnala che l'istanza EC2 elencata o un container nel tuo ambiente AWS eseguono una query su un nome di dominio associato a un'attività correlata a Bitcoin o a un'altra criptovaluta. Gli autori delle minacce potrebbero cercare di assumere il controllo delle risorse di calcolo al fine di riutilizzarle in modo dannoso per il mining non autorizzato di criptovalute.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se utilizzi questa istanza EC2 o container per estrarre o gestire criptovaluta o se questi elementi sono altrimenti coinvolti nell'attività di blockchain, l'esito CryptoCurrency:Runtime/BitcoinTool.B!DNS potrebbe essere un'attività prevista per il tuo ambiente. Se questo è il caso nel tuo AWS ambiente, ti

consigliamo di impostare una regola di soppressione per questo risultato. La regola di eliminazione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `CryptoCurrency:Runtime/BitcoinTool.B!DNS`. Il secondo criterio di filtro deve essere l'ID istanza dell'istanza o l'ID immagine del container del container coinvolti in attività legate alle criptovalute o alla blockchain. Per ulteriori informazioni, consulta Regole di eliminazione.

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Backdoor:Runtime/C&CActivity.B!DNS

Un'istanza Amazon EC2 o un container eseguono una query su nome di dominio associato a un server di comando e controllo noto.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo esito segnala che l'istanza EC2 elencata o il container all'interno del tuo ambiente AWS eseguono una query su un nome di dominio associato a un server di comando e controllo (C&C) noto. L'istanza EC2 elencata o il container potrebbero essere compromessi. I server di comando e controllo sono computer che inviano comandi ai membri di una botnet.

Una botnet è una raccolta di dispositivi connessi a Internet, come PC, server, dispositivi mobili e dispositivi Internet of Things, che sono infettati e controllati da un tipo comune di malware. Le botnet sono spesso utilizzate per distribuire malware e rubare informazioni sensibili, ad esempio i numeri di carte di credito. A seconda dello scopo e della struttura della botnet, il server C&C potrebbe anche inviare comandi per lanciare un attacco DDoS (Distributed Denial of Service).

> **Note**
>
> Se il nome di dominio su cui è stata eseguita la query è relativo a log4j, i campi dell'esito associato includeranno i valori seguenti:
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

> **Note**
>
> Per verificare come GuardDuty genera questo tipo di risultato, puoi effettuare una richiesta DNS dalla tua istanza (utilizzando `dig` per Linux o `nslookup` per Windows) su un dominio di test. `guarddutyc2activityb.com`

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Trojan:Runtime/BlackholeTraffic!DNS

Un'istanza Amazon EC2 o un container eseguono una query su un nome di dominio che è reindirizzato a un indirizzo IP di un buco nero.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo esito segnala che l'istanza EC2 elencata o il container nel tuo ambiente AWS potrebbero essere compromessi in quanto eseguono una query su un nome di dominio che è reindirizzato all'indirizzo IP di un buco nero. I buchi neri sono zone della rete dove il traffico in entrata e in uscita viene eliminato silenziosamente senza che l'origine venga informata del mancato recapito dei dati al destinatario.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Trojan:Runtime/DropPoint!DNS

Un'istanza Amazon EC2 o un container eseguono una query su un nome di dominio di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che un'istanza EC2 o un contenitore nel tuo AWS ambiente sta interrogando il nome di dominio di un host remoto noto per contenere credenziali e altri dati rubati catturati dal malware.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Trojan:Runtime/DGADomainRequest.C!DNS

Un'istanza Amazon EC2 o un container eseguono una query su domini generati da algoritmi. Tali domini sono in genere utilizzati da malware e potrebbero essere un'indicazione di un'istanza EC2 o un container compromessi.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo esito segnala che l'istanza EC2 elencata o il container nel tuo ambiente AWS tentano di eseguire una query su domini DGA. La risorsa potrebbe essere stata compromessa.

I DGA sono utilizzati periodicamente per generare un gran numero di nomi di dominio che possono essere utilizzati come punti di incontro con i relativi server di comando e controllo (C&C). I server

di comando e controllo sono computer che inviano comandi a membri di una botnet, ovvero una raccolta di dispositivi connessi a Internet infettati e controllati da un tipo comune di malware. Il numero elevato di punti di rendez-vous potenziali rende difficile l'arresto delle botnet in quanto i computer infettati tentano di contattare quotidianamente alcuni di questi nomi di dominio per ricevere aggiornamenti o comandi.

> **Note**
>
> Questa scoperta si basa su domini DGA noti provenienti dai feed di intelligence sulle GuardDuty minacce.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Trojan:Runtime/DriveBySourceTraffic!DNS

Un'istanza Amazon EC2 o un container eseguono una query su un nome di dominio di un host remoto che è l'origine nota di attacchi di download drive-by.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo esito segnala che l'istanza EC2 elencata o il container nel tuo ambiente AWS potrebbero essere compromessi in quanto eseguono una query su un nome di dominio di un host remoto che è un'origine nota di attacchi di download drive-by. Si tratta di download di software non voluti da Internet che possono avviare l'installazione automatica di virus, spyware o malware.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Trojan:Runtime/PhishingDomainRequest!DNS

Un'istanza Amazon EC2 o un container eseguono una query su domini implicati in attacchi di phishing.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo esito segnala che nel tuo ambiente AWS sono presenti un'istanza EC2 o un container che tentano di eseguire una query su un dominio implicato in attacchi di phishing. I domini di phishing sono configurati da individui che fingono di essere un'istituzione legittima allo scopo di indurre gli utenti a fornire dati sensibili come informazioni personali, coordinate bancarie, informazioni di carte di credito e password. L'istanza EC2 o il container potrebbero tentare di recuperare dati sensibili archiviati su un sito Web di phishing oppure di configurare un sito Web di phishing. L'istanza EC2 o il container potrebbero essere compromessi.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Impact:Runtime/AbusedDomainRequest.Reputation

Un'istanza Amazon EC2 o un container eseguono una query su un nome di dominio a bassa reputazione associato a domini noti in abuso.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo esito segnala che l'istanza EC2 elencata o il container all'interno del tuo ambiente AWS eseguono una query su un nome di dominio a bassa reputazione associato a domini o indirizzi IP noti in abuso. Esempi di domini in abuso sono i nomi di dominio di primo livello (TLD) e i nomi di dominio di secondo livello (2LD) che offrono registrazioni gratuite di sottodomini e provider DNS dinamici. Gli autori delle minacce tendono a utilizzare questi servizi per registrare domini gratuitamente o a basso costo. I domini a bassa reputazione di questa categoria possono anche essere domini scaduti che vengono sostituiti con l'indirizzo IP di parcheggio di un registrar e quindi potrebbero non essere più attivi. Un IP di parcheggio è il luogo in cui un registrar indirizza il traffico verso domini che non sono stati collegati ad alcun servizio. L'istanza Amazon EC2 elencata o il container potrebbero essere compromessi poiché gli autori delle minacce utilizzano comunemente questi registrar o servizi per la distribuzione di malware e C&C.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Impact:Runtime/BitcoinDomainRequest.Reputation

Un'istanza Amazon EC2 o un container eseguono una query su un nome di dominio a bassa reputazione associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo esito segnala che l'istanza EC2 elencata o il container all'interno del tuo ambiente AWS eseguono una query su un nome di dominio a bassa reputazione associato a un'attività correlata a Bitcoin o a un'altra criptovaluta. Gli autori delle minacce potrebbero cercare di assumere il controllo delle risorse di calcolo per riutilizzarle in modo dannoso per il mining non autorizzato di criptovalute.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se utilizzi questa istanza EC2 o il container per estrarre o gestire criptovaluta o se tali risorse sono altrimenti coinvolte nell'attività di blockchain, questo esito potrebbe rappresentare un'attività prevista per il tuo ambiente. Se questo è il caso nel tuo AWS ambiente, ti consigliamo di impostare una regola di soppressione per questo risultato. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio di filtro deve utilizzare l'attributo Tipo di risultato con un valore di `Impact:Runtime/BitcoinDomainRequest.Reputation`. Il secondo criterio di filtro deve essere l'ID istanza dell'istanza o l'ID immagine del container del container coinvolti in attività legate alle criptovalute o alla blockchain. Per ulteriori informazioni, consulta Regole di eliminazione.

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Impact:Runtime/MaliciousDomainRequest.Reputation

Un'istanza Amazon EC2 o un container eseguono una query su un dominio a bassa reputazione associato a domini dannosi noti.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo esito segnala che l'istanza EC2 elencata o il container all'interno del tuo ambiente AWS eseguono una query su un nome di dominio a bassa reputazione associato a domini o indirizzi IP dannosi noti. Ad esempio, i domini possono essere associati a un indirizzo IP sinkhole noto. I domini sinkhole sono domini che sono stati precedentemente controllati da un autore di minacce e se vengono inoltrate richieste a questi domini può significare che l'istanza è compromessa. Questi domini possono anche essere correlati a campagne dannose note o algoritmi di generazione di domini.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Impact:Runtime/SuspiciousDomainRequest.Reputation

Un'istanza Amazon EC2 o un container eseguono una query su un nome di dominio a bassa reputazione di natura sospetta a causa della sua età o della scarsa popolarità.

Gravità predefinita: bassa

- Funzionalità: monitoraggio del runtime

Questo esito segnala che l'istanza EC2 elencata o il container nel tuo ambiente AWS eseguono una query su un nome di dominio a bassa reputazione sospettato di essere dannoso. Abbiamo notato che le caratteristiche di questo dominio erano coerenti con i domini dannosi osservati in precedenza, ma il nostro modello di reputazione non è stato in grado di collegarlo in modo definitivo a una minaccia nota. Questi domini vengono in genere osservati per la prima volta o ricevono una quantità di traffico ridotta.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

UnauthorizedAccess:Runtime/MetadataDNSRebind

Un'istanza Amazon EC2 o un container eseguono ricerche DNS che vengono risolte nel servizio di metadati dell'istanza.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

> **Note**
>
> Attualmente, questo tipo di ricerca è supportato solo per l'architettura AMD64.

Questo risultato ti informa che un'istanza EC2 o un contenitore nel tuo AWS ambiente sta interrogando un dominio che si risolve nell'indirizzo IP dei metadati EC2 (169.254.169.254). Una query DNS di questo tipo può indicare che l'istanza è la destinazione di una tecnica di rebinding DNS. Questa tecnica può essere utilizzata per ottenere metadati da un'istanza EC2, incluse le credenziali IAM a essa associate.

Il rebinding DNS implica l'inganno di un'applicazione in esecuzione sull'istanza EC2 per caricare i dati restituiti da un URL, dove il nome di dominio nell'URL si risolve nell'indirizzo IP dei metadati EC2 (`169.254.169.254`). In questo modo l'applicazione accede ai metadati EC2 e, possibilmente, li rende disponibili all'utente malintenzionato.

Puoi accedere ai metadati EC2 utilizzando il rebinding DNS solo se l'istanza EC2 esegue un'applicazione vulnerabile che consente l'iniezione di URL oppure se qualcuno accede all'URL in un browser Web in esecuzione sull'istanza EC2.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

In risposta a questo esito, devi valutare se è presente un'applicazione vulnerabile in esecuzione sull'istanza EC2 o sul container o se qualcuno ha utilizzato un browser per accedere al dominio identificato nell'esito. Se la causa principale è un'applicazione vulnerabile, procedi alla correzione

della vulnerabilità. Se qualcuno ha navigato nel dominio identificato, blocca il dominio o impedisci agli utenti di accedervi. Se ritieni che l'esito sia correlato a uno dei due casi precedenti, Revoca la sessione associata all'istanza EC2.

Alcuni AWS clienti associano intenzionalmente l'indirizzo IP dei metadati a un nome di dominio sui propri server DNS autoritativi. Se questo è il caso del tuo ambiente , ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio di filtro deve utilizzare l'attributo Tipo di risultato con un valore di `UnauthorizedAccess:Runtime/MetaDataDNSRebind`. Il secondo criterio di filtro deve essere il Dominio richiesta DNS o l'ID immagine del container. Il valore del Dominio richiesta DNS deve corrispondere al dominio mappato all'indirizzo IP dei metadati (`169.254.169.254`). Per informazioni sulla creazione di regole di eliminazione, consulta Regole di eliminazione.

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Execution:Runtime/NewBinaryExecuted

È stato eseguito un file binario appena creato o modificato di recente in un container.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo esito segnala che è stato eseguito un file binario appena creato o modificato di recente in un container. Ti consigliamo di mantenere i container non modificabili in fase di runtime. Inoltre, i file binari, gli script e le librerie non devono essere creati o modificati durante il ciclo di vita del container. Questo comportamento indica che un malintenzionato che ha ottenuto l'accesso al contenitore ha scaricato ed eseguito malware o altro software come parte della potenziale compromissione. Sebbene questo tipo di attività possa essere indice di una compromissione, è anche un modello di utilizzo comune. Pertanto, GuardDuty utilizza meccanismi per identificare i casi sospetti di questa attività e genera questo tipo di risultati solo per i casi sospetti.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

PrivilegeEscalation:Runtime/DockerSocketAccessed

Un processo all'interno di un container comunica con il daemon Docker utilizzando il socket Docker.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Il socket Docker è un socket di dominio Unix utilizzato da daemon Docker (`dockerd`) per comunicare con i propri client. Un client può eseguire varie operazioni, come la creazione di container comunicando con il daemon Docker tramite il socket Docker. È sospetto che un processo del container acceda al socket Docker. Un processo del container può sfuggire ad esso e ottenere un accesso a livello di host comunicando con il socket Docker e creando un container privilegiato.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

PrivilegeEscalation:Runtime/RuncContainerEscape

È stato rilevato un tentativo di ottenere l'accesso all'host di un container.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo esito segnala che il file binario runC dell'host è stato potenzialmente sovrascritto. RunC è il runtime del container di basso livello utilizzato dai runtime dei container di alto livello, come

Docker e Containerd, per generare ed eseguire container. RunC viene sempre eseguito con privilegi root perché deve effettuare un'operazione di basso livello, ossia la creazione di un container. Una vulnerabilità [1] ben nota in passato consentiva ai container dannosi di sovrascrivere il file binario RunC dell'host e di ottenere l'accesso a livello di root all'host quando veniva eseguito il binario RunC modificato.

Questo esito può anche indicare che un utente malintenzionato ha potenzialmente eseguito un comando in uno dei due tipi di container seguenti:

- Un nuovo container con un'immagine controllata dall'utente malintenzionato.
- Un container esistente che in precedenza era accessibile all'utente malintenzionato con autorizzazioni di scrittura.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

- 1. Dettagli CVE-2019-5736

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

È stata rilevata un'evasione da un container tramite runC in un cluster Amazon EKS.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo esito segnala che è stato rilevato un tentativo di modificare un file dell'agente di rilascio del gruppo di controllo (cgroup). Linux utilizza i gruppi di controllo (cgroup) per limitare, tenere in considerazione e isolare l'utilizzo delle risorse di una raccolta di processi. Ogni cgroup ha un file dell'agente di rilascio (`release_agent`), uno script che Linux esegue quando termina un processo

all'interno del cgroup. Il file dell'agente di rilascio viene sempre eseguito a livello di host. Un autore di minacce all'interno di un container può sfuggire all'host scrivendo comandi arbitrari nel file dell'agente di rilascio che appartiene a un cgroup. Al termine di un processo all'interno di questo cgroup, i comandi scritti dall'autore vengono eseguiti.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.Proc

In un container o in un'istanza Amazon EC2 è stata rilevata un'iniezione di processo utilizzando il file system proc.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

L'iniezione di processo è una tecnica utilizzata dagli autori delle minacce per iniettare codice nei processi in modo da eludere le difese e cercare di aumentare i privilegi. Il file system proc (procfs) è un particolare file system in Linux che presenta la memoria virtuale del processo come file. Il percorso di questo file è `/proc/PID/mem`, in cui `PID` è l'ID univoco del processo. Un autore di minacce può scrivere su questo file per iniettare codice nel processo. Questo esito identifica potenziali tentativi di scrittura sul file in questione.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il tipo di risorsa potrebbe essere stato compromesso. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.Ptrace

In un container o in un'istanza Amazon EC2 è stata rilevata un'iniezione di processo utilizzando la chiamata di sistema ptrace.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

L'iniezione di processo è una tecnica utilizzata dagli autori delle minacce per iniettare codice nei processi in modo da eludere le difese e cercare di aumentare i privilegi. Un processo può utilizzare la chiamata di sistema ptrace per iniettare codice in un altro processo. Questo esito identifica un potenziale tentativo di iniettare codice in un processo utilizzando la chiamata di sistema ptrace.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il tipo di risorsa potrebbe essere stato compromesso. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

In un container o in un'istanza Amazon EC2 è stata rilevata un'iniezione di processo tramite scrittura diretta nella memoria virtuale.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

L'iniezione di processo è una tecnica utilizzata dagli autori delle minacce per iniettare codice nei processi in modo da eludere le difese e cercare di aumentare i privilegi. Un processo può utilizzare una chiamata di sistema, ad esempio `process_vm_writev`, per iniettare codice direttamente nella memoria virtuale di un altro processo. Questo esito identifica un potenziale tentativo di iniettare

codice in un processo utilizzando una chiamata di sistema per scrivere nella memoria virtuale del processo stesso.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il tipo di risorsa potrebbe essere stato compromesso. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Execution:Runtime/ReverseShell

Un processo in un container o in un'istanza Amazon EC2 ha creato una shell (interprete di comandi) inversa.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Una shell (interprete di comandi) inversa è una sessione di shell creata su una connessione avviata dall'host di destinazione all'host dell'attore, ossia l'opposto di una normale shell (interprete di comandi), che viene invece avviata dall'host dell'attore all'host di destinazione. Gli autori delle minacce creano una shell (interprete di comandi) inversa per eseguire comandi sulla destinazione dopo aver ottenuto l'accesso iniziale. Questo esito identifica un potenziale tentativo di creare una shell (interprete di comandi) inversa.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il tipo di risorsa potrebbe essere stato compromesso.

DefenseEvasion:Runtime/FilelessExecution

Un processo in un container o in un'istanza Amazon EC2 esegue codice dalla memoria.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo esito segnala un processo eseguito utilizzando un file eseguibile in memoria su disco. Si tratta di una tecnica comune di evasione della difesa in cui il file eseguibile dannoso non viene scritto sul disco per eludere il rilevamento basato sulla scansione del file system. Sebbene questa sia una tecnica utilizzata dal malware, presenta anche alcuni casi d'uso legittimi. Uno degli esempi è un compilatore just-in-time (JIT) che scrive codice compilato in memoria e lo esegue dalla memoria.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Impact:Runtime/CryptoMinerExecuted

Un container o un'istanza Amazon EC2 eseguono un file binario associato a un'attività attività di mining di criptovalute.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che un contenitore o un'istanza EC2 nel tuo AWS ambiente sta eseguendo un file binario associato a un'attività di mining di criptovalute. Gli autori delle minacce potrebbero cercare di assumere il controllo delle risorse di calcolo per riutilizzarle in modo dannoso per il mining non autorizzato di criptovalute.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console e vediCorrezione dei risultati del Runtime Monitoring.

Execution:Runtime/NewLibraryLoaded

Una libreria appena creata o modificata di recente è stata caricata da un processo all'interno di un container.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo esito segnala che una libreria è stata creata o modificata all'interno di un container durante il runtime e caricata da un processo in esecuzione all'interno del container. La best practice è quella di mantenere i container non modificabili in fase di runtime e di non creare o modificare i file binari, gli script e le librerie durante il ciclo di vita del container. Il caricamento di una libreria appena creata o modificata in un container può indicare attività sospette. Questo comportamento indica che un utente malintenzionato ha potenzialmente ottenuto l'accesso al container e che ha scaricato ed eseguito malware o altro software come parte della potenziale compromissione. Sebbene questo tipo di attività possa essere indice di un compromesso, è anche un modello di utilizzo comune. Pertanto, GuardDuty utilizza meccanismi per identificare i casi sospetti di questa attività e genera questo tipo di risultati solo per i casi sospetti.

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

Un processo all'interno di un container ha montato un file system host in fase di runtime.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Diverse tecniche di evasione da un container prevedono il montaggio di un file system host al suo interno in fase di runtime. Questo esito segnala che un processo all'interno di un container ha potenzialmente tentato di montare un file system host, il che potrebbe indicare un tentativo di sfuggire all'host.

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

PrivilegeEscalation:Runtime/UserfaultfdUsage

Un processo ha utilizzato chiamate di sistema **`userfaultfd`** per gestire errori di pagina nello spazio utente.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

In genere, gli errori di pagina vengono gestiti dal kernel nello spazio corrispondente. Tuttavia, la chiamata di sistema `userfaultfd` consente a un processo di gestire gli errori di pagina su un file system nello spazio utente. Questa funzionalità è utile perché abilita l'implementazione di file system nello spazio utente. D'altra parte, può anche essere usata da un processo potenzialmente dannoso per interrompere il kernel dallo spazio utente. L'interruzione del kernel tramite la chiamata di sistema `userfaultfd` è una tecnica di sfruttamento comune volta a estendere le finestre di gara durante lo sfruttamento delle condizioni di gara del kernel. L'utilizzo di `userfaultfd` può quindi indicare attività sospette sull'istanza Amazon Elastic Compute Cloud (Amazon EC2).

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Execution:Runtime/SuspiciousTool

Un contenitore o un'istanza Amazon EC2 esegue un file o uno script binario che viene spesso utilizzato in scenari di sicurezza offensivi come il pentesting engagement.

Gravità predefinita: variabile

La gravità di questo risultato può essere elevata o bassa, a seconda che lo strumento sospetto rilevato sia considerato a duplice uso o destinato esclusivamente a un uso offensivo.

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che uno strumento sospetto è stato eseguito su un'istanza o contenitore EC2 all'interno del tuo ambiente. AWS Ciò include gli strumenti utilizzati negli interventi di pentesting, noti anche come strumenti di backdoor, scanner di rete e sniffer di rete. Tutti questi strumenti possono essere utilizzati in contesti benigni, ma sono spesso utilizzati anche da autori di minacce con intenti malevoli. L'osservazione di strumenti di sicurezza offensivi potrebbe indicare che l'istanza o il contenitore EC2 associato è stato compromesso.

GuardDuty esamina l'attività e il contesto di runtime correlati in modo da generare questo risultato solo quando l'attività e il contesto associati sono potenzialmente sospetti.

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Execution:Runtime/SuspiciousCommand

Un comando sospetto è stato eseguito su un'istanza Amazon EC2 o su un contenitore che è indicativo di una compromissione.

Gravità predefinita: variabile

A seconda dell'impatto del pattern dannoso osservato, la gravità di questo tipo di rilevamento potrebbe essere bassa, media o alta.

- Funzionalità: monitoraggio del runtime

Questo risultato indica che è stato eseguito un comando sospetto e indica che un'istanza Amazon EC2 o un contenitore nel AWS tuo ambiente è stato compromesso. Ciò potrebbe significare che un file è stato scaricato da una fonte sospetta e quindi eseguito oppure che un processo in esecuzione mostra uno schema dannoso noto nella riga di comando. Ciò indica inoltre che sul sistema è in esecuzione del malware.

GuardDuty esamina l'attività e il contesto di runtime correlati in modo da generare questo risultato solo quando l'attività e il contesto associati sono potenzialmente sospetti.

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

DefenseEvasion:Runtime/SuspiciousCommand

È stato eseguito un comando sull'istanza Amazon EC2 o su un contenitore elencato, tenta di modificare o disabilitare un meccanismo di difesa Linux, come un firewall o servizi di sistema essenziali.

Gravità predefinita: variabile

A seconda del meccanismo di difesa modificato o disabilitato, la gravità di questo tipo di risultato può essere alta, media o bassa.

- Funzionalità: monitoraggio del runtime

Questa scoperta indica che è stato eseguito un comando che tenta di nascondere un attacco ai servizi di sicurezza del sistema locale. Ciò include azioni come la disabilitazione del firewall Unix, la modifica delle tabelle IP locali, la rimozione di crontab voci, la disabilitazione di un servizio locale o l'assunzione della funzione. `LDPreload` Qualsiasi modifica è altamente sospetta e rappresenta un potenziale indicatore di compromissione. Pertanto, questi meccanismi rilevano o impediscono ulteriori compromissioni del sistema.

GuardDuty esamina l'attività e il contesto di runtime correlati in modo da generare questo risultato solo quando l'attività e il contesto associati sono potenzialmente sospetti.

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nei dettagli dei risultati nella console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

DefenseEvasion:Runtime/PtraceAntiDebugging

Un processo in un contenitore o in un'istanza Amazon EC2 ha eseguito una misura anti-debug utilizzando la chiamata di sistema ptrace.

Gravità predefinita: bassa

- Funzionalità: monitoraggio del runtime

Questo risultato mostra che un processo in esecuzione su un'istanza Amazon EC2 o su un contenitore all'interno del tuo AWS ambiente ha utilizzato la chiamata di sistema ptrace con l'opzione. `PTRACE_TRACEME` Questa attività provocherebbe il distacco di un debugger collegato dal processo in esecuzione. Se non è collegato alcun debugger, non ha alcun effetto. Tuttavia, l'attività di per sé solleva sospetti. Ciò potrebbe indicare che sul sistema è in esecuzione del malware. Il malware utilizza spesso tecniche anti-debug per eludere l'analisi e queste tecniche possono essere rilevate in fase di esecuzione.

GuardDuty esamina l'attività e il contesto di runtime correlati in modo da generare questo risultato solo quando l'attività e il contesto associati sono potenzialmente sospetti.

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Execution:Runtime/MaliciousFileExecuted

Un file eseguibile dannoso noto è stato eseguito su un'istanza o un contenitore Amazon EC2.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che un file eseguibile dannoso noto è stato eseguito su un'istanza Amazon EC2 o su un contenitore all'interno AWS del tuo ambiente. Si tratta di un forte indicatore del fatto che l'istanza o il contenitore sono stati potenzialmente compromessi e che il malware è stato eseguito.

Il malware utilizza spesso tecniche anti-debugging per eludere l'analisi e queste tecniche possono essere rilevate in fase di esecuzione.

GuardDuty esamina l'attività e il contesto di runtime correlati in modo da generare questo risultato solo quando l'attività e il contesto associati sono potenzialmente sospetti.

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

GuardDuty Tipi di ricerca S3

I seguenti risultati sono specifici per le risorse di Amazon S3 e avranno un tipo di risorsa **`S3Bucket`** se l'origine CloudTrail dati è data events per S3 o **`AccessKey`** se l'origine dati è CloudTrail un evento di gestione. La gravità e i dettagli dei risultati saranno diversi in base al tipo di ricerca e all'autorizzazione associata al bucket.

Gli esiti qui elencati includono le origini dati e i modelli utilizzati per generare quel tipo di esito. Per ulteriori informazioni sulle origini dati e sui modelli, consulta Origini dati fondamentali.

> **Important**
>
> I risultati con una fonte di dati sugli eventi di CloudTrail dati per S3 vengono generati solo se la protezione S3 è abilitata per. GuardDuty La Protezione S3 è abilitata per impostazione predefinita in tutti gli account creati dopo il 31 luglio 2020. Per informazioni su come abilitare o disabilitare la Protezione S3, consulta Protezione Amazon S3 su Amazon GuardDuty

Per tutti i tipi di esiti `S3Bucket`, ti consigliamo di esaminare le autorizzazioni sul bucket in questione e le autorizzazioni di tutti gli utenti coinvolti nell'esito. Se l'attività è non è prevista, consulta le raccomandazioni per la correzione descritte in dettaglio in Riparazione di un bucket S3 potenzialmente compromesso.

Argomenti

- 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

Un'API comunemente utilizzata per scovare gli oggetti S3 è stata richiamata in modo anomalo.

Gravità predefinita: bassa

- Fonte dati: eventi relativi CloudTrail ai dati per S3

Questo esito indica che un'entità IAM ha richiamato un'API S3 per scoprire i bucket S3 nel tuo ambiente, ad esempio `ListObjects`. Questo tipo di attività è associato alla fase di scoperta di un attacco in cui l'utente malintenzionato raccoglie informazioni per determinare se il tuo ambiente AWS è suscettibile a un attacco più ampio. Questa attività è sospetta perché l'entità IAM ha richiamato l'API in un modo insolito. Ad esempio, un'entità IAM senza cronologia precedente richiama un'API S3 o un'entità IAM richiama un'API S3 da una posizione insolita.

Questa API è stata identificata come anomala dal modello ML (Anomaly Detection Machine Learning) GuardDuty di Anomaly Detection. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Tiene traccia di vari fattori delle richieste API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'API specifica e il bucket richiesti e il numero di chiamate API effettuate. Per ulteriori informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta, consulta Dettagli sui risultati.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Discovery:S3/MaliciousIPCaller

Un'API S3 comunemente utilizzata per scovare risorse in un ambiente AWS è stata richiamata da un indirizzo IP dannoso noto.

Gravità predefinita: alta

- Fonte dei dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'operazione API S3 è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata alla fase di scoperta di un attacco, quando un avversario raccoglie informazioni sul tuo ambiente AWS. A titolo di esempio si possono menzionare `GetObjectAcl` e `ListObjects`.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Discovery:S3/MaliciousIPCaller.Custom

Un'API S3 è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: alta

- Fonte dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'API S3, come `GetObjectAcl` o `ListObjects`, è stata richiamata da un indirizzo IP incluso in un elenco minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. Questo tipo di attività è associato alla fase di scoperta di un attacco in cui l'utente malintenzionato raccoglie informazioni per determinare se il tuo ambiente AWS è suscettibile a un attacco più ampio.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Discovery:S3/TorIPCaller

Un'API S3 è stata richiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: media

- Fonte dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'API S3, come `GetObjectAcl` o `ListObjects`, è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. Questo tipo di attività è associato alla fase di scoperta di un attacco in cui l'utente malintenzionato raccoglie informazioni per determinare se il tuo ambiente AWS è suscettibile a un attacco più ampio. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle risorse AWS con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Exfiltration:S3/AnomalousBehavior

Un'entità IAM ha richiamato un'API S3 in modo sospetto.

Gravità predefinita: alta

- Fonte dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'entità IAM effettua chiamate API che coinvolgono un bucket S3 e questa attività differisce dalla linea di base stabilita per tale entità. La chiamata API utilizzata in questa attività è associata alla fase di esfiltrazione di un attacco, in cui un utente malintenzionato tenta di raccogliere dati. Questa attività è sospetta perché l'entità IAM ha richiamato l'API in un modo insolito. Ad esempio, un'entità IAM senza cronologia precedente richiama un'API S3 o un'entità IAM richiama un'API S3 da una posizione insolita.

Questa API è stata identificata come anomala dal modello ML (Anomaly Detection Machine Learning) GuardDuty di Anomaly Detection. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Tiene traccia di vari fattori delle richieste API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata,

l'API specifica e il bucket richiesti e il numero di chiamate API effettuate. Per ulteriori informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta, consulta Dettagli sui risultati.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Exfiltration:S3/MaliciousIPCaller

Un'API S3 comunemente utilizzata per raccogliere dati da un ambiente AWS è stata richiamata da un indirizzo IP dannoso noto.

Gravità predefinita: alta

- Fonte dei dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'operazione API S3 è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata a tattiche di esfiltrazione in cui un avversario cerca di raccogliere dati dalla tua rete. A titolo di esempio si possono menzionare `GetObject` e `CopyObject`.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Impact:S3/AnomalousBehavior.Delete

Un'entità IAM ha richiamato un'API S3 che tenta di eliminare i dati in modo sospetto.

Gravità predefinita: alta

- Fonte dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'entità IAM nel tuo ambiente AWS effettua chiamate API che coinvolgono un bucket S3 e questo comportamento differisce dalla linea di base stabilita per tale entità. La chiamata API utilizzata in questa attività è associata a un attacco che tenta di eliminare i dati. Questa attività è sospetta perché l'entità IAM ha richiamato l'API in un modo insolito. Ad esempio, un'entità IAM senza cronologia precedente richiama un'API S3 o un'entità IAM richiama un'API S3 da una posizione insolita.

Questa API è stata identificata come anomala dal modello ML (Anomaly Detection Machine Learning) GuardDuty di Anomaly Detection. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Tiene traccia di vari fattori delle richieste API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'API specifica e il bucket richiesti e il numero di chiamate API effettuate. Per ulteriori informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta, consulta Dettagli sui risultati.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Ti consigliamo di controllare il contenuto del tuo bucket S3 per determinare se la versione precedente dell'oggetto può o deve essere ripristinata.

Impact:S3/AnomalousBehavior.Permission

Un'API comunemente utilizzata per impostare le autorizzazioni della lista di controllo degli accessi (ACL) è stata richiamata in modo anomalo.

Gravità predefinita: alta

- Fonte dei dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'entità IAM nel tuo ambiente AWS ha modificato una policy o un'ACL sui bucket S3 elencati. Tale modifica può esporre pubblicamente i bucket S3 a tutti gli utenti AWS autenticati.

Questa API è stata identificata come anomala dal modello ML (Anomaly Detection Machine Learning) GuardDuty di Anomaly Detection. Il modello di ML valuta tutte le richieste API nel tuo account e

identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Tiene traccia di vari fattori delle richieste API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'API specifica e il bucket richiesti e il numero di chiamate API effettuate. Per ulteriori informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta, consulta Dettagli sui risultati.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Ti consigliamo di controllare il contenuto del tuo bucket S3 per assicurarti che a nessun oggetto sia stato inaspettatamente consentito l'accesso pubblico.

Impact:S3/AnomalousBehavior.Write

Un'entità IAM ha richiamato un'API S3 che tenta di scrivere i dati in modo sospetto.

Gravità predefinita: media

- Fonte dei dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'entità IAM nel tuo ambiente AWS effettua chiamate API che coinvolgono un bucket S3 e questo comportamento differisce dalla linea di base stabilita per tale entità. La chiamata API utilizzata in questa attività è associata a un attacco che tenta di scrivere i dati. Questa attività è sospetta perché l'entità IAM ha richiamato l'API in un modo insolito. Ad esempio, un'entità IAM senza cronologia precedente richiama un'API S3 o un'entità IAM richiama un'API S3 da una posizione insolita.

Questa API è stata identificata come anomala dal modello ML (Anomaly Detection Machine Learning) GuardDuty di Anomaly Detection. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Tiene traccia di vari fattori delle richieste API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'API specifica e il bucket richiesti e il numero di chiamate API effettuate. Per ulteriori informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta, consulta Dettagli sui risultati.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Ti consigliamo di controllare il contenuto del tuo bucket S3 per assicurarti che questa chiamata API non abbia scritto dati dannosi o non autorizzati.

Impact:S3/MaliciousIPCaller

Un'API S3 comunemente utilizzata per manomettere dati o processi in un ambiente AWS è stata richiamata da un indirizzo IP dannoso noto.

Gravità predefinita: alta

- Fonte dei dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'operazione API S3 è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata a tattiche di impatto con cui un avversario cerca di manipolare, interrompere o distruggere dati all'interno del tuo ambiente AWS. A titolo di esempio si possono menzionare `PutObject` e `PutObjectAcl`.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

PenTest:S3/KaliLinux

Un'API S3 è stata richiamata da una macchina Kali Linux.

Gravità predefinita: media

- Fonte dati: eventi di CloudTrail dati per S3

Questo esito segnala che una macchina in cui è in esecuzione Kali Linux sta effettuando chiamate API S3 utilizzando credenziali che appartengono al tuo account AWS. Le tue credenziali potrebbero

essere compromesse. Kali Linux è uno noto strumento per l'esecuzione di test di intrusione utilizzato dai professionisti della sicurezza informatica per identificare le vulnerabilità nelle istanze EC2 che richiedono l'applicazione di patch. Questo strumento è utilizzato anche dagli utenti malintenzionati per identificare le vulnerabilità nella configurazione EC2 e ottenere accesso non autorizzato all'ambiente AWS.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

PenTest:S3/ParrotLinux

Un'API S3 è stata richiamata da una macchina Parrot Security Linux.

Gravità predefinita: media

- Fonte dati: eventi di CloudTrail dati per S3

Questo esito segnala che una macchina in cui è in esecuzione Parrot Security Linux sta effettuando chiamate API S3 utilizzando credenziali che appartengono al tuo account AWS. Le tue credenziali potrebbero essere compromesse. Parrot Security Linux è uno noto strumento per l'esecuzione di test di intrusione utilizzato dai professionisti della sicurezza informatica per identificare le vulnerabilità nelle istanze EC2 che richiedono l'applicazione di patch. Questo strumento è utilizzato anche dagli utenti malintenzionati per identificare le vulnerabilità nella configurazione EC2 e ottenere accesso non autorizzato all'ambiente AWS.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

PenTest:S3/PentooLinux

Un'API S3 è stata richiamata da una macchina Pentoo Linux.

Gravità predefinita: media

- Fonte dati: eventi di CloudTrail dati per S3

Questo esito segnala che una macchina in cui è in esecuzione Pentoo Linux sta effettuando chiamate API S3 utilizzando credenziali che appartengono al tuo account AWS. Le tue credenziali potrebbero essere compromesse. Pentoo Linux è uno noto strumento per l'esecuzione di test di intrusione utilizzato dai professionisti della sicurezza informatica per identificare le vulnerabilità nelle istanze EC2 che richiedono l'applicazione di patch. Questo strumento è utilizzato anche dagli utenti malintenzionati per identificare le vulnerabilità nella configurazione EC2 e ottenere accesso non autorizzato all'ambiente AWS.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Policy:S3/AccountBlockPublicAccessDisabled

Un'entità IAM ha richiamato un'API utilizzata per disabilitare il blocco dell'accesso pubblico S3 su un account.

Gravità predefinita: bassa

- Fonte dei dati: eventi CloudTrail di gestione

Questo esito segnala che il blocco dell'accesso pubblico Amazon S3 è stato disabilitato a livello di account. Quando le impostazioni relative al blocco dell'accesso pubblico S3 sono abilitate, vengono utilizzate per filtrare le policy o le liste di controllo degli accessi (ACL) sui bucket come misura di sicurezza per evitare l'esposizione pubblica accidentale dei dati.

In genere, il blocco dell'accesso pubblico S3 è disattivato nell'account per consentire l'accesso pubblico a un bucket o agli oggetti al suo interno. Quando il blocco dell'accesso pubblico S3 è disabilitato per un account, l'accesso ai bucket è controllato dalle policy, dalle ACL o dalle impostazioni di blocco dell'accesso pubblico a livello di bucket applicate ai singoli bucket. Questo

non significa per forza che i bucket sono condivisi pubblicamente, ma che è necessario controllare le autorizzazioni applicate ai bucket per verificare che forniscano il livello di accesso appropriato.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Policy:S3/BucketAnonymousAccessGranted

Un principale IAM ha concesso l'accesso a Internet a un bucket S3 modificando le policy o le ACL del bucket.

Gravità predefinita: alta

- Fonte dei dati: eventi CloudTrail di gestione

Questo esito segnala che il bucket S3 elencato è stato reso accessibile pubblicamente su Internet perché un'entità IAM ha modificato una policy o un'ACL per il bucket in questione. Una volta rilevata una modifica alla policy o all'ACL, viene utilizzato il ragionamento automatico fornito da Zelkova per determinare se il bucket è accessibile pubblicamente.

> **Note**
>
> Se le ACL o le policy del bucket sono configurate per negare esplicitamente o negare tutto, questo esito potrebbe non riflettere lo stato attuale del bucket. Questo esito non rifletterà alcuna impostazione di Blocco dell'accesso pubblico S3 che potrebbe essere stata abilitata per il tuo bucket S3. In questi casi, il valore `effectivePermission` dell'esito verrà contrassegnato come `UNKNOWN`.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Policy:S3/BucketBlockPublicAccessDisabled

Un'entità IAM ha richiamato un'API utilizzata per disabilitare il blocco dell'accesso pubblico S3 su un bucket.

Gravità predefinita: bassa

- Fonte dei dati: eventi CloudTrail di gestione

Questo esito segnala che il blocco dell'accesso pubblico è stato disabilitato per il bucket S3 elencato. Quando sono abilitate, le impostazioni relative al blocco dell'accesso pubblico S3 vengono utilizzate per filtrare le policy o le liste di controllo degli accessi (ACL) applicate ai bucket come misura di sicurezza per evitare l'esposizione pubblica accidentale dei dati.

In genere, il blocco dell'accesso pubblico S3 è disattivato su un bucket per consentire l'accesso pubblico al bucket in questione o agli oggetti al suo interno. Quando il blocco dell'accesso pubblico S3 è disabilitato per un bucket, l'accesso al bucket stesso è controllato dalle relative policy o ACL. Questo non significa che il bucket è condiviso pubblicamente, ma è necessario controllare le policy e le ACL applicate al bucket per verificare che vengano applicate le autorizzazioni appropriate.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Policy:S3/BucketPublicAccessGranted

Un principale IAM ha concesso l'accesso pubblico a un bucket S3 da parte di tutti gli utenti AWS modificando le policy o le ACL del bucket.

Gravità predefinita: alta

- Fonte dei dati: eventi CloudTrail di gestione

Questo esito segnala che il bucket S3 elencato è stato esposto pubblicamente a tutti gli utenti AWS autenticati perché un'entità IAM ha modificato una policy o un'ACL per il bucket S3 in questione. Una

volta rilevata una modifica alla policy o all'ACL, viene utilizzato il ragionamento automatico fornito da Zelkova per determinare se il bucket è accessibile pubblicamente.

> **Note**
>
> Se le ACL o le policy del bucket sono configurate per negare esplicitamente o negare tutto, questo esito potrebbe non riflettere lo stato attuale del bucket. Questo esito non rifletterà alcuna impostazione di Blocco dell'accesso pubblico S3 che potrebbe essere stata abilitata per il tuo bucket S3. In questi casi, il valore `effectivePermission` dell'esito verrà contrassegnato come `UNKNOWN`.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Stealth:S3/ServerAccessLoggingDisabled

La registrazione degli accessi al server S3 è stata disabilitata per un bucket.

Gravità predefinita: bassa

- Fonte dei dati: eventi CloudTrail di gestione

Questo esito segnala che la registrazione degli accessi al server S3 è disabilitata per un bucket all'interno del tuo ambiente AWS. Se disabilitata, non viene creato alcun registro delle richieste Web per i tentativi di accesso al bucket S3 identificato, tuttavia, le chiamate API di gestione S3 al bucket, ad esempio, vengono comunque tracciate DeleteBucket. Se la registrazione degli eventi dei dati S3 è abilitata CloudTrail per questo bucket, le richieste web per gli oggetti all'interno del bucket verranno comunque tracciate. La disabilitazione della registrazione è una tecnica utilizzata da utenti non autorizzati per evitare il rilevamento. Per ulteriori informazioni sui log S3, consulta Registrazione degli accessi al server S3 e Opzioni di registrazione S3 .

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

Un'API S3 è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: alta

- Fonte dati: eventi di dati per S3 CloudTrail

Questo esito segnala che un'operazione API S3, ad esempio, `PutObject` o `PutObjectAcl`, è stata richiamata da un indirizzo IP incluso in un elenco minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

UnauthorizedAccess:S3/TorIPCaller

Un'API S3 è stata richiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: alta

- Fonte dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'operazione API S3, come `PutObject` o `PutObjectAcl`, è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. L'esito può indicare un accesso non autorizzato alle risorse AWS con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Tipi di esiti ritirati

Un esito è una notifica che contiene dettagli su un potenziale problema di sicurezza rilevato da GuardDuty. Per informazioni su importanti modifiche apportate ai tipi di risultati di GuardDuty, tra cui tipi di risultati recentemente aggiunti o ritirati, consulta Cronologia dei documenti per Amazon GuardDuty.

I seguenti tipi di esiti sono stati ritirati e non vengono più generati da GuardDuty.

> **Important**
>
> Non puoi riattivare i tipi di esiti ritirati di GuardDuty.

Argomenti

- 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

Exfiltration:S3/ObjectRead.Unusual

Un'entità IAM ha richiamato un'API S3 in modo sospetto.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

- Origine dati: eventi di dati di CloudTrail per S3

Questo esito segnala che un'entità IAM nel tuo ambiente AWS effettua chiamate API che coinvolgono un bucket S3 e che differiscono dalla linea di base stabilita per tale entità. La chiamata API utilizzata in questa attività è associata alla fase di esfiltrazione di un attacco, in cui un utente malintenzionato tenta di raccogliere dati. Questa attività è sospetta perché il modo in cui l'entità IAM ha richiamato l'API è insolito. Ad esempio, l'entità IAM non aveva mai richiamato questo tipo di API in precedenza oppure l'API è stata richiamata da una posizione insolita.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Impact:S3/PermissionsModification.Unusual

Un'entità IAM ha richiamato un'API per modificare le autorizzazioni su una o più risorse S3.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito segnala che un'entità IAM effettua chiamate API progettate per modificare le autorizzazioni su uno o più bucket o oggetti nel tuo ambiente AWS. Questa operazione può essere eseguita da un utente malintenzionato per consentire la condivisione di informazioni al di fuori dell'account. Questa attività è sospetta perché il modo in cui l'entità IAM ha richiamato l'API è insolito. Ad esempio, l'entità IAM non aveva mai richiamato questo tipo di API in precedenza oppure l'API è stata richiamata da una posizione insolita.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Impact:S3/ObjectDelete.Unusual

Un'entità IAM ha richiamato un'API utilizzata per eliminare i dati in un bucket S3.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito indica che un'entità IAM specifica nel tuo ambiente AWS effettua chiamate API progettate per eliminare i dati nel bucket S3 elencato tramite l'eliminazione del bucket stesso. Questa attività è sospetta perché il modo in cui l'entità IAM ha richiamato l'API è insolito. Ad esempio, l'entità IAM non aveva mai richiamato questo tipo di API in precedenza oppure l'API è stata richiamata da una posizione insolita.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Discovery:S3/BucketEnumeration.Unusual

Un'entità IAM ha richiamato un'API S3 utilizzata per scoprire i bucket S3 all'interno della rete.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito indica che un'entità IAM ha richiamato un'API S3 per scoprire i bucket S3 nel tuo ambiente, ad esempio `ListBuckets`. Questo tipo di attività è associato alla fase di scoperta di un attacco in cui l'utente malintenzionato raccoglie informazioni per determinare se il tuo ambiente AWS è suscettibile a un attacco più ampio. Questa attività è sospetta perché il modo in cui l'entità IAM ha richiamato l'API è insolito. Ad esempio, l'entità IAM non aveva mai richiamato questo tipo di API in precedenza oppure l'API è stata richiamata da una posizione insolita.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Persistence:IAMUser/NetworkPermissions

Un'entità IAM ha richiamato un'API comunemente utilizzata per modificare le autorizzazioni di accesso alla rete per gruppi di sicurezza, instradamenti e ACL nel tuo account AWS.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito segnala che un principale specifico (Utente root dell'account AWS, ruolo IAM o utente) nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita. Questa entità di sicurezza non ha mai chiamato questa API in precedenza.

Questo esito viene attivato quando le impostazioni di configurazione della rete vengono modificate in circostanze sospette, ad esempio quando un principale richiama l'API `CreateSecurityGroup` senza averlo mai fatto in precedenza. Gli utenti malintenzionati spesso tentano di modificare i gruppi di sicurezza per consentire un determinato traffico in entrata su varie porte e migliorare la capacità di accedere all'istanza EC2.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Persistence:IAMUser/ResourcePermissions

Un principale ha richiamato un'API comunemente utilizzata per modificare le policy di accesso di varie risorse nel tuo Account AWS.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito segnala che un principale specifico (Utente root dell'account AWS, ruolo IAM o utente) nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita. Questa entità di sicurezza non ha mai chiamato questa API in precedenza.

Questo esito viene attivato quando viene rilevata una modifica alle policy o alle autorizzazioni collegate alle risorse AWS, ad esempio quando un principale nel tuo ambiente AWS richiama l'API `PutBucketPolicy` senza averlo mai fatto in precedenza. Alcuni servizi, come Amazon S3, supportano le autorizzazioni collegate alle risorse che concedono a uno o più principali di accedere alla risorsa. Con le credenziali rubate, gli utenti malintenzionati possono modificare le policy collegate a una risorsa per potervi accedere.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Persistence:IAMUser/UserPermissions

Un principale ha richiamato un'API comunemente utilizzata per aggiungere, modificare o eliminare utenti, gruppi o policy IAM nel tuo account AWS.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito segnala che un principale specifico (Utente root dell'account AWS, ruolo IAM o utente) nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita. Questa entità di sicurezza non ha mai chiamato questa API in precedenza.

Questo esito viene attivato da modifiche sospette apportate alle autorizzazioni collegate agli utenti nel tuo ambiente AWS, ad esempio quando un principale dell'ambiente AWS richiama l'API `AttachUserPolicy` senza averlo mai fatto in precedenza. Gli utenti malintenzionati possono utilizzare le credenziali rubate per creare nuovi utenti, aggiungere policy di accesso agli utenti esistenti o creare chiavi di accesso per massimizzare l'accesso a un account, anche se il punto di accesso originale è chiuso. Ad esempio, il proprietario dell'account potrebbe accorgersi del furto di un determinato utente IAM o di una password ed eliminarli dall'account. Tuttavia, potrebbe non eliminare altri utenti creati da un principale amministratore creato in modo fraudolento, lasciando il loro account AWS accessibile all'utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

PrivilegeEscalation:IAMUser/AdministrativePermissions

Un principale ha tentato di assegnare una policy molto permissiva a se stessa.

Gravità predefinita: bassa*

> **Note**
>
> La gravità di questo esito è bassa se il tentativo di escalation dei privilegi non è andato a buon fine e media in caso contrario.

Questo esito indica che un'entità IAM specifica nel tuo ambiente AWS ha un comportamento che può essere indicativo di un attacco di escalation dei privilegi. Questo esito viene attivato quando un utente o un ruolo IAM tentano di autoassegnarsi una policy molto permissiva. Se l'utente o il ruolo in questione non intende godere di privilegi amministrativi, le credenziali dell'utente possono essere state compromesse o le autorizzazioni del ruolo potrebbero non essere configurate correttamente.

Gli utenti malintenzionati utilizzeranno le credenziali rubate per creare nuovi utenti, aggiungere policy di accesso agli utenti esistenti o creare chiavi di accesso per massimizzare l'accesso a un account, anche se il punto di accesso originale è chiuso. Ad esempio, il proprietario dell'account potrebbe notare che una determinata credenziale di un utente IAM è stata rubata ed eliminata dall'account, ma potrebbe non eliminare altri utenti creati da un principale amministratore creato in modo fraudolento, lasciando i loro account AWS ancora accessibili all'utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Recon:IAMUser/NetworkPermissions

Un principale ha richiamato un'API comunemente utilizzata per modificare le autorizzazioni di accesso alla rete per gruppi di sicurezza, instradamenti e ACL nel tuo account AWS.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito segnala che un principale specifico (Utente root dell'account AWS, ruolo IAM o utente) nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita. Questa entità di sicurezza non ha mai chiamato questa API in precedenza.

Questo esito viene attivato quando le autorizzazioni di accesso alle risorse nel tuo AWS sono sottoposte a probing in circostanze sospette. Ad esempio, se un principale ha richiamato l'API `DescribeInstances` senza averlo mai fatto in precedenza. Un utente malintenzionato potrebbe utilizzare le credenziali rubate per eseguire questo tipo di ricognizione delle risorse AWS allo scopo di trovare credenziali più utili o determinare le capacità delle credenziali di cui dispone.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Recon:IAMUser/ResourcePermissions

Un principale ha richiamato un'API comunemente utilizzata per modificare le policy di accesso di varie risorse nel tuo account AWS.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito segnala che un principale specifico (Utente root dell'account AWS, ruolo IAM o utente) nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita. Questa entità di sicurezza non ha mai chiamato questa API in precedenza.

Questo esito viene attivato quando le autorizzazioni di accesso alle risorse nel tuo AWS sono sottoposte a probing in circostanze sospette. Ad esempio, se un principale ha richiamato l'API `DescribeInstances` senza averlo mai fatto in precedenza. Un utente malintenzionato potrebbe utilizzare le credenziali rubate per eseguire questo tipo di ricognizione delle risorse AWS allo scopo di trovare credenziali più utili o determinare le capacità delle credenziali di cui dispone.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Recon:IAMUser/UserPermissions

Un principale ha richiamato un'API comunemente utilizzata per aggiungere, modificare o eliminare utenti, gruppi o policy IAM nel tuo account AWS.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito viene attivato quando le autorizzazioni utente nel tuo ambiente AWS sono sottoposte a probing in circostanze sospette. Ad esempio, se un principale (Utente root dell'account AWS, ruolo IAM o utente IAM) ha richiamato l'API `ListInstanceProfilesForRole` senza averlo mai fatto in precedenza. Un utente malintenzionato potrebbe utilizzare le credenziali rubate per eseguire

questo tipo di ricognizione delle risorse AWS allo scopo di trovare credenziali più utili o determinare le capacità delle credenziali di cui dispone.

Questo esito indica che un principale specifico nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita. Questo primcipal non ha mai chiamato questa API in precedenza.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

ResourceConsumption:IAMUser/ComputeResources

Un principale ha chiamato un'API comunemente utilizzata per avviare risorse di calcolo come istanze EC2.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito viene generato quando le istanze EC2 nell'account elencato all'interno del tuo ambiente AWS vengono avviate in circostanze sospette. Questo esito indica che un principale specifico nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita, ad esempio se un principale (Utente root dell'account AWS, ruolo IAM o utente IAM) nel tuo ambiente ha richiamato l'API `RunInstances` senza averlo mai fatto in precedenza. Questa attività potrebbe essere un'indicazione che un utente malintenzionato sta utilizzando credenziali rubate per rubare tempo di calcolo (possibilmente per il mining di criptovalute o il password cracking). Può anche essere la prova che un utente malintenzionato sta utilizzando un'istanza EC2 nel tuo ambiente AWS e le relative credenziali per mantenere l'accesso al tuo account.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Stealth:IAMUser/LoggingConfigurationModified

Un principale ha richiamato un'API comunemente utilizzata per interrompere la registrazione CloudTrail, eliminare i log esistenti o eliminare tracce di attività nel tuo account AWS.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito viene attivato quando la configurazione della registrazione nell'account AWS elencato all'interno del tuo ambiente viene modificata in circostanze sospette. Questo esito segnala che un principale specifico nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita, ad esempio se un principale (Utente root dell'account AWS, ruolo IAM o utente IAM) nel tuo ambiente ha richiamato l'API `StopLogging` senza averlo mai fatto in precedenza. Ciò può indicare il tentativo di un utente malintenzionato di eliminare le tracce della sua attività.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

UnauthorizedAccess:IAMUser/ConsoleLogin

È stato osservato un accesso insolito alla console da parte di un principale nel tuo account AWS.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo risultato viene generato quando una connessione alla console viene rilevata in circostanze sospette. Ad esempio, se un principale che non ha mai chiamato l'API ConsoleLogin in precedenza, lo fa da un client mai utilizzato o da una posizione inabituale. Ciò potrebbe indicare l'utilizzo di credenziali rubate per accedere al tuo account AWS oppure l'accesso da parte di un utente valido all'account in un modo non valido o meno sicuro (ad esempio, non tramite una VPN approvata).

Questo esito segnala che un principale specifico nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita. Questo principale non ha mai eseguito connessioni con questa applicazione client da questo specifico percorso in precedenza.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

UnauthorizedAccess:EC2/TorIPCaller

Un'istanza EC2 sta ricevendo connessioni in entrata da un nodo di uscita Tor.

Gravità predefinita: media

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS riceve connessioni in entrata da un nodo di uscita Tor. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relè tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. L'esito può indicare un accesso non autorizzato alle risorse AWS con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Backdoor:EC2/XORDDOS

Un'istanza EC2 sta tentando di comunicare con un indirizzo IP associato a malware XOR DDoS.

Gravità predefinita: alta

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS sta tentando di comunicare con un indirizzo IP associato a malware XOR DDoS. L'istanza EC2 potrebbe essere compromessa.

XOR DDoS è un trojan che assume il controllo dei sistemi Linux. Per accedere al sistema, lancia un attacco di forza bruta allo scopo di scoprire la password dei servizi SSH (Secure Shell) su Linux. Dopo aver ottenuto le credenziali SSH ed effettuato la connessione, utilizza privilegi utente root per eseguire uno script che scarica e installa XOR DDoS. Questo malware viene in seguito utilizzato in una botnet per lanciare attacchi DDoS (Distributed Denial of Service) contro altri target.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

Behavior:IAMUser/InstanceLaunchUnusual

Un utente ha avviato un tipo insolito di istanza EC2.

Gravità predefinita: alta

Questo esito segnala che un utente specifico nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita. Questo utente non ha mai avviato un'istanza EC2 di questo tipo in precedenza. Le tue credenziali di accesso potrebbero essere compromesse.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

CryptoCurrency:EC2/BitcoinTool.A

Un'istanza EC2 sta comunicando con pool di mining di bitcoin.

Gravità predefinita: alta

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS sta comunicando con pool di mining di Bitcoin. Nel settore del mining di criptovalute, un pool di mining designa il raggruppamento delle risorse dei minatori che condividono la loro potenza di elaborazione su una rete per condividere la ricompensa in funzione del loro contributo alla risoluzione di un blocco. Se l'istanza EC2 non è utilizzata per il mining di bitcoin, potrebbe essere compromessa.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

UnauthorizedAccess:IAMUser/UnusualASNCaller

Un'API è stata chiamata da un indirizzo IP di una rete inabituale.

Gravità predefinita: alta

Questo risultato segnala che un'attività è stata chiamata da un indirizzo IP di una rete inabituale. Questa rete non è mai stata osservata nello storico di utilizzo di AWS dell'utente specificato. Questa attività può includere una accesso alla console, un tentativo di avviare un'istanza EC2, di creare un nuovo utente IAM, di modificare i privilegi AWS, ecc. Ciò può indicare un accesso non autorizzato alle risorse AWS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Esiti per tipo di risorsa

Le pagine seguenti sono suddivise in categorie per tipo di risorsa associata a un GuardDuty risultato:

- Tipi di esiti EC2
- Tipi di risultati del monitoraggio del runtime
- Tipi di esiti IAM
- Tipi di esiti dei log di audit di Kubernetes
- Tipi di esiti della Protezione Lambda
- Tipi di esiti della protezione da malware
- Tipi di esiti della Protezione RDS
- Tipi di esiti S3

Tabella degli esiti

La tabella seguente mostra tutti i tipi di esiti attivi ordinati per origine dati o funzionalità fondamentale, a seconda dei casi. Alcuni dei seguenti tipi di esiti possono avere diversi livelli di gravità, indicati da un asterisco (*). Per informazioni sulla gravità variabile di un tipo di esito, visualizza la descrizione dettagliata corrispondente.

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Discovery:S3/AnomalousBehavior	Amazon S3	CloudTrail eventi di dati per S3	Bassa
Discovery:S3/MaliciousIPCaller	Amazon S3	CloudTrail eventi di dati per S3	Elevata
Discovery:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail eventi di dati per S3	Elevata
Discovery:S3/TorIPCaller	Amazon S3	CloudTrail eventi di dati per S3	Media
Exfiltration:S3/AnomalousBehavior	Amazon S3	CloudTrail eventi di dati per S3	Elevata
Exfiltration:S3/MaliciousIPCaller	Amazon S3	CloudTrail eventi di dati per S3	Elevata
Impact:S3/AnomalousBehavior.Delete	Amazon S3	CloudTrail eventi di dati per S3	Elevata
Impact:S3/AnomalousBehavior.Permission	Amazon S3	CloudTrail eventi di dati per S3	Elevata
Impact:S3/Anomalou	Amazon S3	CloudTrail eventi di dati per S3	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
sBehavior.Write			
Impact:S3/MaliciousIPCaller	Amazon S3	CloudTrail eventi di dati per S3	Elevata
PenTest:S3/KaliLinux	Amazon S3	CloudTrail eventi di dati per S3	Media
PenTest:S3/ParrotLinux	Amazon S3	CloudTrail eventi di dati per S3	Media
PenTest:S3/PentooLinux	Amazon S3	CloudTrail eventi di dati per S3	Media
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	CloudTrail eventi di dati per S3	Elevata
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail eventi di dati per S3	Elevata
CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail evento di gestione	Media
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail evento di gestione	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail evento di gestione	Bassa
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail evento di gestione	Elevata
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail evento di gestione	Elevata
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail evento di gestione	Media
PenTest:IAMUser/KaliLinux	IAM	CloudTrail evento di gestione	Media
PenTest:IAMUser/ParrotLinux	IAM	CloudTrail evento di gestione	Media
PenTest:IAMUser/PentooLinux	IAM	CloudTrail evento di gestione	Media
Persistence:IAMUser/AnomalousBehavior	IAM	CloudTrail evento di gestione	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Stealth:IAMUser/PasswordPolicyChange	IAM	CloudTrail evento di gestione	Basso*
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	IAM	CloudTrail evento di gestione	Alta*
Policy:S3/AccountBlockPublicAccessDisabled	Amazon S3	CloudTrail evento di gestione	Bassa
Policy:S3/BucketAnonymousAccessGranted	Amazon S3	CloudTrail evento di gestione	Elevata
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	CloudTrail evento di gestione	Bassa
Policy:S3/BucketPublicAccessGranted	Amazon S3	CloudTrail evento di gestione	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	CloudTrail evento di gestione	Media
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail evento di gestione	Media
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail evento di gestione	Media
Recon:IAMUser/TorIPCaller	IAM	CloudTrail evento di gestione	Media
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail evento di gestione	Bassa
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	CloudTrail evento di gestione	Bassa
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail evento di gestione	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail evento di gestione	Media
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail evento di gestione	Media
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail evento di gestione	Media
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail eventi di gestione o eventi CloudTrail relativi ai dati per S3	Bassa
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail eventi di gestione o eventi CloudTrail relativi ai dati per S3	Elevata
Backdoor:EC2/C&CActivity.B!DNS	Amazon EC2	Log DNS	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	Log DNS	Elevata
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	Log DNS	Media
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	Log DNS	Elevata
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	Log DNS	Elevata
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	Log DNS	Bassa
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	Log DNS	Media
Trojan:EC2/DGADomainRequest.B	Amazon EC2	Log DNS	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	Log DNS	Elevata
Trojan:EC2/DNSDataExfiltration	Amazon EC2	Log DNS	Elevata
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	Log DNS	Elevata
Trojan:EC2/DropPoint!DNS	Amazon EC2	Log DNS	Media
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	Log DNS	Elevata
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	Log DNS	Elevata
Execution:Container/MaliciousFile	Container	Volumi EBS	Varia a seconda della minaccia rilevata
Execution:Container/SuspiciousFile	Container	Volumi EBS	Varia a seconda della minaccia rilevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Execution:EC2/MaliciousFile	EC2	Volumi EBS	Varia a seconda della minaccia rilevata
Execution:EC2/SuspiciousFile	EC2	Volumi EBS	Varia a seconda della minaccia rilevata
Execution:ECS/MaliciousFile	ECS	Volumi EBS	Varia a seconda della minaccia rilevata
Execution:ECS/SuspiciousFile	ECS	Volumi EBS	Varia a seconda della minaccia rilevata
Execution:Kubernetes/MaliciousFile	Kubernetes	Volumi EBS	Varia a seconda della minaccia rilevata
Execution:Kubernetes/SuspiciousFile	Kubernetes	Volumi EBS	Varia a seconda della minaccia rilevata
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	Log di audit di Kubernetes	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	Log di audit di Kubernetes	Elevata
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log di audit di Kubernetes	Elevata
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log di audit di Kubernetes	Elevata
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	Log di audit di Kubernetes	Elevata
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	Log di audit di Kubernetes	Elevata
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log di audit di Kubernetes	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log di audit di Kubernetes	Elevata
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	Log di audit di Kubernetes	Elevata
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	Log di audit di Kubernetes	Bassa
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	Log di audit di Kubernetes	Media
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log di audit di Kubernetes	Media
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log di audit di Kubernetes	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Discovery:Kubernetes/TorIPCaller	Kubernetes	Log di audit di Kubernetes	Media
Execution:Kubernetes/ExecInKubeSystemPod	Kubernetes	Log di audit di Kubernetes	Media
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	Log di audit di Kubernetes	Media
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	Log di audit di Kubernetes	Bassa
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	Log di audit di Kubernetes	Elevata
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log di audit di Kubernetes	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log di audit di Kubernetes	Elevata
Impact:Kubernetes/TorIPCaller	Kubernetes	Log di audit di Kubernetes	Elevata
Persistence:Kubernetes/ContainerWithSensitiveMount	Kubernetes	Log di audit di Kubernetes	Media
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	Log di audit di Kubernetes	Media
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Log di audit di Kubernetes	Media
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Log di audit di Kubernetes	Elevata
Persistence:Kubernetes/TorIPCaller	Kubernetes	Log di audit di Kubernetes	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	Log di audit di Kubernetes	Elevata
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	Log di audit di Kubernetes	Elevata
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	Log di audit di Kubernetes	Media
Policy:Kubernetes/ExposedDashboard	Kubernetes	Log di audit di Kubernetes	Media
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	Kubernetes	Log di audit di Kubernetes	Medio*

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	Kubernetes	Log di audit di Kubernetes	Bassa
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	Log di audit di Kubernetes	Elevata
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	Log di audit di Kubernetes	Elevata
PrivilegeEscalation:Kubernetes/PrivilegedContainer	Kubernetes	Log di audit di Kubernetes	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Backdoor:Lambda/C&CActivity.B	Lambda	Monitoraggio delle attività di rete Lambda	Elevata
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Monitoraggio delle attività di rete Lambda	Elevata
Trojan:Lambda/BlackholeTraffic	Lambda	Monitoraggio delle attività di rete Lambda	Media
Trojan:Lambda/DropPoint	Lambda	Monitoraggio delle attività di rete Lambda	Media
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Monitoraggio delle attività di rete Lambda	Media
UnauthorizedAccess:Lambda/TorClient	Lambda	Monitoraggio delle attività di rete Lambda	Elevata
UnauthorizedAccess:Lambda/TorRelay	Lambda	Monitoraggio delle attività di rete Lambda	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	Database Amazon Aurora supportati	Monitoraggio delle attività di accesso RDS	Bassa
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	Database Amazon Aurora supportati	Monitoraggio delle attività di accesso RDS	Elevata
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	Database Amazon Aurora supportati	Monitoraggio delle attività di accesso RDS	Variabile*
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	Database Amazon Aurora supportati	Monitoraggio delle attività di accesso RDS	Media
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	Database Amazon Aurora supportati	Monitoraggio delle attività di accesso RDS	Elevata
CredentialAccess:RDS/TorIPCaller.FailedLogin	Database Amazon Aurora supportati	Monitoraggio delle attività di accesso RDS	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	Database Amazon Aurora supportati	Monitoraggio delle attività di accesso RDS	Elevata
Discovery:RDS/MaliciousIPCaller	Database Amazon Aurora supportati	Monitoraggio delle attività di accesso RDS	Media
Discovery:RDS/TorIPCaller	Database Amazon Aurora supportati	Monitoraggio delle attività di accesso RDS	Media
Backdoor:Runtime/C&CActivity.B	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
Backdoor:Runtime/C&CActivity.B!DNS	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
CryptoCurrency:Runtime/BitcoinTool.B	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
CryptoCurrency:Runtime/BitcoinTool.B!DNS	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
DefenseEvasion:Runtime/FilelessExecution	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
DefenseEvasion:Runtime/ProcessInjection.Proc	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
DefenseEvasion:Runtime/ProcessInjection.Ptrace	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
DefenseEvasion:Runtime/PtraceAntiDebugging	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Bassa
DefenseEvasion:Runtime/SuspiciousCommand	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
Execution:Runtime/MaliciousFileExecuted	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
Execution:Runtime/NewBinaryExecuted	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Execution:Runtime/NewLibraryLoaded	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
Execution:Runtime/SuspiciousCommand	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Variabile
Execution:Runtime/SuspiciousTool	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Variabile
Execution:Runtime/ReverseShell	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
Impact:Runtime/AbusedDomainRequest.Reputation	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
Impact:Runtime/BitcoinDomainRequest.Reputation	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
Impact:Runtime/CryptoMinerExecuted	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Impact:Runtime/MaliciousDomainRequest.Reputation	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
Impact:Runtime/SuspiciousDomainRequest.Reputation	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Bassa
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
PrivilegeEscalation:Runtime/DockerSocketAccessed	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
PrivilegeEscalation:Runtime/RuncContainerEscape	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
PrivilegeEscalation:Runtime/UserfaultfdUsage	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
Trojan:Runtime/BlackholeTraffic	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
Trojan:Runtime/BlackholeTraffic!DNS	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
Trojan:Runtime/DropPoint	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
Trojan:Runtime/DGADomainRequest.C!DNS	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
Trojan:Runtime/DriveBySourceTraffic!DNS	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Trojan:Runtime/DropPoint!DNS	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Media
Trojan:Runtime/PhishingDomainRequest!DNS	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
UnauthorizedAccess:Runtime/MetadataDNSRebind	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
UnauthorizedAccess:Runtime/TorClient	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
UnauthorizedAccess:Runtime/TorRelay	Istanza, cluster EKS, cluster ECS o contenitore	Monitoraggio del runtime	Elevata
Backdoor:EC2/C&CActivity.B	EC2	Log di flusso VPC	Elevata
Backdoor:EC2/DenialOfService.Dns	EC2	Log di flusso VPC	Elevata
Backdoor:EC2/DenialOfService.Tcp	EC2	Log di flusso VPC	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Backdoor:EC2/DenialOfService.Udp	EC2	Log di flusso VPC	Elevata
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	EC2	Log di flusso VPC	Elevata
Backdoor:EC2/DenialOfService.UnusualProtocol	EC2	Log di flusso VPC	Elevata
Backdoor:EC2/Spambot	EC2	Log di flusso VPC	Media
Behavior:EC2/NetworkPortUnusual	EC2	Log di flusso VPC	Media
Behavior:EC2/TrafficVolumeUnusual	EC2	Log di flusso VPC	Media
CryptoCurrency:EC2/BitcoinTool.B	EC2	Log di flusso VPC	Elevata
DefenseEvasion:EC2/UnusualDNSResolver	EC2	Log di flusso VPC	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
DefenseEvasion:EC2/UnusualDoHActivity	EC2	Log di flusso VPC	Media
DefenseEvasion:EC2/UnusualDoTActivity	EC2	Log di flusso VPC	Media
Impact:EC2/PortSweep	EC2	Log di flusso VPC	Elevata
Impact:EC2/WinRMBruteForce	EC2	Log di flusso VPC	Basso*
Recon:EC2/PortProbeEMRUnprotectedPort	EC2	Log di flusso VPC	Elevata
Recon:EC2/PortProbeUnprotectedPort	EC2	Log di flusso VPC	Basso*
Recon:EC2/Portscan	EC2	Log di flusso VPC	Media
Trojan:EC2/BlackholeTraffic	EC2	Log di flusso VPC	Media
Trojan:EC2/DropPoint	EC2	Log di flusso VPC	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	EC2	Log di flusso VPC	Media
UnauthorizedAccess:EC2/RDPBruteForce	EC2	Log di flusso VPC	Basso*
UnauthorizedAccess:EC2/SSHBruteForce	EC2	Log di flusso VPC	Basso*
UnauthorizedAccess:EC2/TorClient	EC2	Log di flusso VPC	Elevata
UnauthorizedAccess:EC2/TorRelay	EC2	Log di flusso VPC	Elevata

Gestione dei GuardDuty risultati di Amazon

GuardDuty offre diverse funzioni importanti per aiutarti a ordinare, archiviare e gestire i risultati. Queste funzionalità ti consentono di personalizzare gli esiti in base al tuo ambiente. In questo modo ridurrai il rumore derivante da risultati di basso valore e potrai concentrarti sulle minacce al tuo ambiente AWS . Consulta gli argomenti di questa pagina per capire come utilizzare queste funzionalità per aumentare il valore GuardDuty dei risultati.

Argomenti:

Pannello di riepilogo

Scopri i componenti della dashboard di riepilogo disponibile nella GuardDuty console.

Filtro dei risultati

Scopri come filtrare GuardDuty i risultati in base ai criteri da te specificati.

Regole di eliminazione

Scopri come filtrare automaticamente GuardDuty gli avvisi relativi ai risultati tramite regole di soppressione. Le regole di eliminazione archiviano automaticamente gli esiti a seconda dei filtri impostati.

Utilizzo di elenchi di indirizzi IP affidabili ed elenchi minacce

Personalizza l'ambito del GuardDuty monitoraggio utilizzando elenchi di IP ed elenchi di minacce basati su indirizzi IP instradabili pubblicamente. Gli elenchi di IP affidabili impediscono la generazione di risultati non DNS a partire da IP che consideri affidabili, mentre Threat Intel Lists ti avviserà delle attività provenienti GuardDuty da IP definiti dall'utente.

Esportazione degli esiti

Esporta i risultati generati in un bucket Amazon S3 in modo da poter conservare i record oltre il periodo di conservazione dei risultati di 90 giorni. GuardDuty Utilizza questi dati storici per tenere traccia delle potenziali attività sospette nel tuo account e valutare se le misure correttive consigliate hanno avuto successo.

Creazione di risposte personalizzate ai GuardDuty risultati con Amazon CloudWatch Events

Imposta notifiche automatiche per GuardDuty i risultati tramite Amazon CloudWatch Events. Puoi anche automatizzare altre attività tramite CloudWatch Events per aiutarti a rispondere ai risultati.

Comprensione CloudWatch dei log e dei motivi per cui le risorse vengono ignorate durante la scansione di Malware Protection

Scopri come controllare CloudWatch Logs for GuardDuty Malware Protection e quali sono i motivi per cui l'istanza Amazon EC2 o i volumi Amazon EBS interessati potrebbero essere stati ignorati durante il processo di scansione.

Segnalazione di falsi positivi nella protezione da malware di GuardDuty

Scopri l'esperienza dei falsi positivi in GuardDuty Malware Protection e come segnalare i rilevamenti di minacce falsi positivi.

Pannello di riepilogo

La dashboard di riepilogo fornisce una visualizzazione aggregata dei GuardDuty risultati generati Account AWS nella regione corrente. Attualmente, il pannello supporta un volume fino a 5.000 esiti. Tuttavia, puoi visualizzare i dettagli di tutti i risultati utilizzando la pagina Findings sulla GuardDuty console GetFindingsoppure ListFindings.

> **Note**
>
> Il riepilogo dei risultati è disponibile solo tramite la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

Le sezioni seguenti consentono di accedere al pannello e di comprenderne i componenti.

Indice

- Accesso al pannello di Riepilogo
- Comprensione del pannello di Riepilogo
- Feedback sul pannello di Riepilogo

Accesso al pannello di Riepilogo

Sulla GuardDuty console, la dashboard di riepilogo mostra una visualizzazione consolidata degli ultimi 5.000 GuardDuty risultati generati nella regione corrente.

Per accedere al pannello di Riepilogo

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Riepilogo. Quando apri la console, GuardDuty mostra la dashboard di riepilogo.
3. Per impostazione predefinita, il riepilogo viene visualizzato per lo stesso giorno, ossia Oggi. La GuardDuty console offre un'opzione per visualizzare il riepilogo degli ultimi 2 giorni, degli ultimi 7 giorni e degli ultimi 30 giorni. Per modificare l'intervallo di tempo predefinito, scegli una delle opzioni dal menu a discesa sopra il riquadro Panoramica.
4. Filtro dei dati

   - I widget Account con il maggior numero di esiti, Risorse con il maggior numero di esiti ed Esiti meno ricorrenti consentono di filtrare i dati in base al livello di gravità degli esiti.
   - Il widget Risorse con il maggior numero di esiti consente inoltre di filtrare i dati in base al tipo di risorsa potenzialmente interessata.

     Un account membro può visualizzare i dettagli della risorsa potenzialmente interessata che appartiene al proprio account. Se sei un account GuardDuty amministratore e desideri visualizzare i dettagli della risorsa potenzialmente interessata, apri la GuardDuty console utilizzando le credenziali dell'account membro associato.
5. Copertura dei piani di protezione

   La copertura dei piani di protezione fornisce il numero di account membri attivati GuardDuty nell'organizzazione. Le statistiche sono visibili solo all' GuardDuty amministratore delegato.

Comprensione del pannello di Riepilogo

Il pannello di Riepilogo mostra i dati aggregati nelle sezioni seguenti. Prima di procedere alla visualizzazione e alla lettura del riepilogo, assicurati di scegliere la Regione AWS desiderata dal selettore della regione nella parte superiore della console. Inoltre, assicurati di scegliere l'intervallo di tempo desiderato dal menu a discesa fornito sopra il riquadro Panoramica. Se non sono stati generati esiti per i parametri scelti, nessun dato sarà disponibile in alcun widget.

Su un volume fino agli ultimi 5.000 GuardDuty risultati, la dashboard di riepilogo con Account con il maggior numero di risultati, Risorse con il maggior numero di risultati e Risultati meno ricorrenti mostra i dati basati sui primi 5 risultati. Per un'analisi più approfondita, consulta la pagina Findings nella GuardDuty console.

Panoramica

Questa sezione fornisce i dati seguenti:

- Esiti totali: indica il numero totale di esiti generati nel tuo account nella regione attuale.
- Risultati di elevata gravità: indica il numero di GuardDuty risultati con un livello di gravità elevato nella regione corrente.
- Risorse con esiti: indica il numero di risorse che sono associate a un esito e che sono state potenzialmente compromesse.
- Account con esiti: indica il numero di account in cui è stato generato almeno un esito. Se sei un account indipendente, il valore di questo campo è 1.

Per gli intervalli di tempo Ultimi 7 giorni e Ultimi 30 giorni, il riquadro Panoramica può mostrare la differenza percentuale rispettivamente degli esiti generati settimanalmente (WoW) o mensilmente (MoM). Se non sono stati generati esiti nella settimana o nel mese precedente, in assenza quindi di dati da confrontare, la differenza percentuale potrebbe non essere disponibile.

Se sei un account GuardDuty amministratore, tutti questi campi forniscono i dati riepilogati di tutti gli account dei membri della tua organizzazione.

Esiti per gravità

Questa sezione mostra un grafico a barre con il numero totale di esiti rispetto all'intervallo di tempo scelto. Puoi visualizzare il numero di esiti con gravità bassa, media o alta generati in una data specifica all'interno dell'intervallo di tempo scelto.

Tipi di esiti più comuni

Questa sezione fornisce un grafico a torta dei cinque principali tipi di risultati più comuni osservati su un volume di fino agli ultimi 5.000 GuardDuty risultati generati nella regione corrente. Questo grafico a torta mostra i seguenti dati quando il puntatore del mouse viene posizionato su ciascun settore:

- Conteggio degli esiti: indica il numero di volte in cui questo esito è stato generato nell'intervallo di tempo selezionato.
- Gravità: indica il livello di gravità dell'esito, ad esempio medio e alto.
- Percentuale: indica la quota di questo tipo di esito nel grafico a torta.
- Ultima generazione: indica quanto tempo è trascorso dall'ultima generazione di questo tipo di esito.

Account con il maggior numero di esiti

Questa sezione fornisce i dati seguenti:

- Account: indica l' Account AWS ID in cui è stato generato il risultato.
- Conteggio dell'esito: indica il numero di volte in cui è stato generato un esito per questo ID account.
- Ultima generazione: indica quanto tempo è trascorso dall'ultima generazione di un tipo di esito per questo ID account.
- Gravità alta: per impostazione predefinita, vengono visualizzati i dati per i tipi di esiti con gravità alta. Le opzioni possibili per questo campo sono Gravità alta, Gravità media e Tutte le gravità.

Risorse con esiti

Questa sezione fornisce i dati seguenti:

- Risorsa: indica il tipo di risorsa potenzialmente interessata e se questa risorsa appartiene al tuo account puoi accedere al collegamento rapido per visualizzarne i dettagli. Se sei un account GuardDuty amministratore, puoi visualizzare i dettagli della risorsa potenzialmente interessata accedendo alla GuardDuty console con le credenziali dell'account membro a cui appartiene questa risorsa.
- Account: indica l' Account AWS ID a cui appartiene questa risorsa.
- Conteggio dell'esito: indica il numero di volte in cui questa risorsa è stata associata a un esito.
- Ultima generazione: indica quanto tempo è trascorso dall'ultima generazione di un tipo di esito associato a questa risorsa.
- Tutti i tipi di risorsa: per impostazione predefinita, i dati vengono visualizzati per tutti i tipi di risorse. Utilizzando il menu a discesa, puoi visualizzare i dati per un tipo di risorsa specifico, come Instance AccessKey, Lambda e altri.
- Gravità alta: per impostazione predefinita, vengono visualizzati i dati per i tipi di esiti con gravità alta. Utilizzando il menu a discesa, puoi visualizzare i dati per altri livelli di gravità. Le opzioni possibili sono Gravità alta, Gravità media e Tutte le gravità.

Esiti meno ricorrenti

Questa sezione fornisce i dettagli dei tipi di risultati che non vengono generati spesso nell'ambiente in uso. AWS Queste informazioni possono essere utili per indagare e agire su un modello di minaccia emergente nel tuo ambiente. La tabella mostra i dati seguenti:

- Tipo di risultato: indica il nome del tipo di esito.
- Conteggio dell'esito: indica il numero di volte in cui questo esito è stato generato nell'intervallo di tempo selezionato.
- Ultima generazione: indica quanto tempo è trascorso dall'ultima generazione di questo tipo di esito.
- Gravità alta: per impostazione predefinita, vengono visualizzati i dati per i tipi di esiti con gravità alta. Le opzioni possibili per questo campo sono Gravità alta, Gravità media e Tutte le gravità.

Copertura dei piani di protezione

Questa sezione fornisce il numero di account membri attivi che appartengono all'organizzazione e che hanno abilitato una o più funzionalità e funzionalità aggiuntive (a seconda dei casi) nella configurazione corrente Regione AWS.

Solo un GuardDuty amministratore delegato può visualizzare le statistiche relative agli account dei membri all'interno della propria organizzazione. Se una funzionalità non è configurata, scegli Configura nella colonna Azioni.

Quando crei una nuova AWS organizzazione, potrebbero essere necessarie fino a 24 ore per generare le statistiche per l'intera organizzazione.

Feedback sul pannello di Riepilogo

GuardDuty ti incoraggia a fornire feedback sull'usabilità, le funzionalità e le prestazioni della dashboard di riepilogo. per sapere come migliorarlo.

Per fornire feedback sul pannello di Riepilogo

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Riepilogo. Quando apri la GuardDuty console, viene visualizzata la dashboard di riepilogo.
3. Scegli Feedback nell'angolo in alto a destra del pannello. Si aprirà un modulo. Dopo aver fornito il feedback, scegli Invia.

Filtro dei risultati

Un filtro per gli esiti ti consente di visualizzare gli esiti che corrispondono ai criteri specificati e di escludere gli esiti non corrispondenti. Puoi creare facilmente filtri di ricerca utilizzando la GuardDuty

console Amazon oppure puoi crearli con l'CreateFilterAPI utilizzando JSON. Consulta le sezioni seguenti per capire come creare un filtro nella console. Per utilizzare questi filtri in modo da archiviare automaticamente gli esiti in arrivo, consulta Regole di eliminazione.

Creazione di filtri nella console GuardDuty

I filtri di ricerca possono essere creati e testati tramite la GuardDuty console. Puoi salvare i filtri che hai creato tramite la console per utilizzarli nelle regole di eliminazione o nelle operazioni di filtro future. Un filtro è composto da almeno un criterio di filtro, che consiste in un attributo del filtro abbinato ad almeno un valore.

Quando crei un nuovo utente, tieni in considerazione quanto segue:

- I filtri non accettano caratteri jolly.
- Puoi specificare da uno a 50 attributi come criteri per un determinato filtro.
- Quando utilizzi la condizione uguale a o non uguale a per filtrare in base a un valore di attributo, ad esempio ID account, puoi specificare un massimo di 50 valori.
- Ogni attributo dei criteri di filtro viene valutato come operatore `AND`. Più valori per lo stesso attributo vengono valutati come `AND/OR`.

Per filtrare i risultati (console)

1. Scegli Aggiungi criteri di filtro sopra l'elenco visualizzato dei GuardDuty risultati.
2. Nell'elenco di attributi espanso, seleziona gli attributi che desideri specificare come criterio di filtro, come ID Account o Tipo di operazione.

   > **Note**
   >
   > Consulta la tabella sugli attributi del filtro in questa pagina per visualizzare un elenco degli attributi che puoi utilizzare per creare criteri di filtro.

3. Nel campo di testo visualizzato, specifica un valore per ogni attributo selezionato, quindi scegli Applica.

> **Note**
>
> Dopo aver applicato un filtro, puoi convertirlo per escludere gli esiti che corrispondono al filtro scegliendo il punto nero a sinistra del nome del filtro. In questo modo viene creato un filtro "non uguale" per l'attributo selezionato.

4. Per salvare gli attributi specificati e i relativi valori (criteri di filtro) come filtro, selezionare Salva. Fornisci il nome e la descrizione del filtro, quindi scegli Fatto.

Attributi del filtro

Quando crei filtri o ordini gli esiti utilizzando le operazioni API, devi specificare i criteri di filtro in JSON. Questi criteri di filtro sono correlati al JSON dei dettagli di un esito. La tabella seguente contiene un elenco dei nomi che vengono visualizzati nella console per gli attributi dei filtri e i nomi dei campi JSON equivalenti.

Nome campo console	Nome campo JSON
ID account	accountId
ID risultato	id
Regione	Regione
Gravità	severity Se utilizzi `severity` con API, AWS CLI o AWS CloudFormation, il relativo valore sarà numerico. Per ulteriori informazioni, consulta findingCriteria.
Tipo di risultato	type
Ora aggiornamento	updatedAt
ID chiave di accesso	risorsa. accessKeyDetails. accessKeyId
ID principale	risorsa. accessKeyDetails. ID principale

Nome campo console	Nome campo JSON
Username	risorsa. accessKeyDetails.Nome utente
Tipo utente	risorsa. accessKeyDetails.tipo di utente
ID profilo dell'istanza IAM	Resource.InstanceDetails. iamInstanceProfile .id
ID istanza	resource.instanceDetails.instanceId
ID immagine istanza	resource.instanceDetails.imageId
Chiave di tag dell'istanza	resource.instanceDetails.tags.key
Valore del tag dell'istanza	resource.instanceDetails.tags.value
Indirizzo IPv6	resource.instanceDetails.networkInterfaces.ip v6Addresses
Indirizzo IPv4 privato	resource.instancedetails.Interfacce di rete. privateIpAddresses. privateIpAddress
Nome DNS pubblico	Resource.InstanceDetails.Interfacce di rete. publicDnsName
IP pubblico	resource.instanceDetails.networkInterfaces.pu blicIp
ID gruppo di sicurezza	resource.instanceDetails.networkInterfaces.se curityGroups.groupId
Nome del gruppo di sicurezza	resource.instanceDetails.networkInterfaces.se curityGroups.groupName
ID sottorete	resource.instanceDetails.networkInterfaces.su bnetId
ID VPC	resource.instanceDetails.networkInterfaces.vp cId

Nome campo console	Nome campo JSON
ARN dell'Outpost	resource.instanceDetails.outpostARN
Tipo di risorsa	resource.resourceType
Autorizzazioni del bucket	resource.s3.publicAccess.EffectivePermission BucketDetails
Nome bucket	risorse.s3 .nome BucketDetails
Chiave tag bucket	risorse.s3 .tags.key BucketDetails
Valore tag bucket	risorse.s3 .tags.value BucketDetails
Tipo bucket	risorse.s3 .type BucketDetails
Tipo di operazione	service.action.actionType
API chiamata	servizio.azione. awsApiCallAzione.api
Tipo intermediario API	servizio.azione. awsApiCallaction.callerType
Codice di errore API	servizio.azione. awsApiCallcodice di errore action.error
Città intermediario API	servizio.azione. awsApiCallAzione. remoteIpDetails.città.Nome della città
Paese intermediario API	servizio.azione. awsApiCallAzione. remoteIpDetails.Paese.CountryName
Indirizzo IPv4 intermediario API	servizio.azione. awsApiCallAzione. remoteIpDetails.Indirizzo IP v4
ID ASN intermediario API	servizio.azione. awsApiCallAzione. remoteIpDetails.organizzazione.asn
Nome ASN intermediario API	servizio.azione. awsApiCallAzione. remoteIpDetails.Organizzazione.asnorg

Nome campo console	Nome campo JSON
Nome del servizio intermediario API	servizio.azione. awsApiCallaction.serviceName
Dominio richiesta DNS	servizio.azione. dnsRequestAction.dominio
Suffisso del dominio richiesta DNS	servizio.azione. dnsRequestAction. domainWithSuffix
Connessione di rete bloccata	servizio.azione. networkConnectionAction.bloccato
Direzione connessione rete	servizio.azione. networkConnectionAction. Direzione della connessione
Porta locale connessione rete	servizio.azione. networkConnectionAction. localPortDetails.porta
Protocollo connessione rete	servizio.azione. networkConnectionAction.protocollo
Città connessione di rete	servizio.azione. networkConnectionAction. remoteIpDetails.città. Nome della città
Paese connessione di rete	servizio.azione. networkConnectionAction. remoteIpDetails.Paese. Nome del Paese
Indirizzo IPv4 remoto connessione rete	servizio.azione. networkConnectionAction. remoteIpDetails.indirizzo IP v4
ID ASN IP remoto connessione rete	servizio.azione. networkConnectionAction. remoteIpDetails.organizzazione.asn
Nome ASN IP remoto connessione rete	servizio.azione. networkConnectionAction. remoteIpDetails.Organizzazione.asnorg
Porta remota connessione rete	servizio.azione. networkConnectionAction. remotePortDetails.porta

Nome campo console	Nome campo JSON
Account remoto affiliato	servizio.azione. awsApiCallAzione. remoteAccountDetails.affiliato
Indirizzo IPv4 chiamante API Kubernetes	servizio.azione. kubernetesApiCallAzione. remoteIpDetails.Indirizzo IP v4
Spazio dei nomi Kubernetes	servizio.azione. kubernetesApiCallAction.namespace
ID ASN chiamante API Kubernetes	servizio.azione. kubernetesApiCallAzione. remoteIpDetails.organizzazione.asn
URI della richiesta di chiamata API Kubernetes	servizio.azione. kubernetesApiCallazione. RequestURI
Codice di stato API Kubernetes	servizio.azione. kubernetesApiCallcodice action.status
Indirizzo IPv4 locale della connessione di rete	servizio.azione. networkConnectionAction. localIpDetails.indirizzo IP v4
Protocollo	servizio.azione. networkConnectionAction.protocollo
Nome servizio chiamata API	servizio.azione. awsApiCallaction.serviceName
ID account chiamante API	servizio.azione. awsApiCallAzione. remoteAccountDetails.ID account
Nome elenco minacce	Servizio. Informazioni aggiuntive. threatListName
Ruolo risorsa	service.resourceRole
Nome del cluster EKS	risorsa. eksClusterDetails.nome
Nome del carico di lavoro Kubernetes	Resource.KubernetesDetails. kubernetesWorkloadDetails.nome

Nome campo console	Nome campo JSON
Spazio dei nomi del carico di lavoro Kubernetes	Resource.KubernetesDetails. kubernetesWorkloadDetails.namespace
Nome utente Kubernetes	Resource.KubernetesDetails. kubernetesUserDetails.nome utente
Immagine del container di Kubernetes	Resource.KubernetesDetails. kubernetesWorkloadDetails.contenitori.immagine
Prefisso dell'immagine del container di Kubernetes	Resource.kubernetesDetails. kubernetesWorkloadDetails.Contenitori.Image Prefix
ID scansione	servizio. ebsVolumeScanDettagli.scanID
Nome minaccia	servizio. ebsVolumeScanDettagli.ScanDetections. threatDetectedByNome.ThreatNames.Name
Gravità delle minacce	servizio. ebsVolumeScanDettagli.ScanDetections. threatDetectedByNome. Nomi delle minacce. Severità
File SHA	servizio. ebsVolumeScanDettagli.ScanDetections. threatDetectedByNome.ThreatNames.FilePaths.Hash
Nome del cluster ECS	risorsa. ecsClusterDetails.nome
Immagine del container ECS	risorsa. ecsClusterDetails.taskdetails.containers.image
ARN di definizione del processo ECS	risorsa. ecsClusterDetails.taskdetails.definitionARN
Immagine del container autonomo	resource.containerDetails.image
ID istanza di database	risorsa. rdsDbInstanceDettagli. dbInstanceIdentifier

Nome campo console	Nome campo JSON
ID del cluster di database	risorsa. rdsDbInstanceDettagli. dbCluster Identifier
Motore di database	risorsa. rdsDbInstanceDettagli.Motore
Utente del database	risorsa. rdsDbUserDettagli. Utente
Chiave di tag dell'istanza database	risorsa. rdsDbInstancedetails.tags.key
Valore del tag dell'istanza database	risorsa. rdsDbInstancedetails.tags.value
SHA-256 eseguibile	service.runtimeDetails.process.executableSha256
Process name (Nome del processo)	service.runtimeDetails.process.name
Percorso eseguibile	service.runtimeDetails.process.executablePath
Nome della funzione Lambda	resource.lambdaDetails.functionName
ARN della funzione Lambda	resource.lambdaDetails.functionArn
Chiave di tag con funzione Lambda	resource.lambdaDetails.tags.key
Valore del tag della funzione lambda	resource.lambdaDetails.tags.value
Dominio richiesta DNS	servizio.azione. dnsRequestAction. domainWithSuffix

Regole di eliminazione

Una regola di eliminazione è un insieme di criteri in cui ogni attributo di filtro è abbinato a un valore. Questi criteri vengono utilizzati per filtrare gli esiti, archiviando automaticamente i nuovi esiti che corrispondono ai criteri specificati. Le regole di soppressione possono essere utilizzate per filtrare risultati di basso valore, risultati falsi positivi o minacce su cui non si intende agire, per facilitare il riconoscimento delle minacce alla sicurezza con l'impatto maggiore sull'ambiente.

Dopo aver creato una regola di soppressione, i nuovi risultati che corrispondono ai criteri definiti nella regola vengono archiviati automaticamente finché la regola di soppressione è in vigore. Puoi utilizzare un filtro esistente per creare una regola di eliminazione oppure puoi crearne una a partire da un nuovo filtro definito. È possibile configurare le regole di eliminazione in modo da eliminare interi tipi di risultati oppure definire criteri di filtro più granulari per sopprimere solo istanze specifiche di un particolare tipo di risultato. Le regole di soppressione possono essere modificate in qualsiasi momento.

I risultati soppressi non vengono inviati ad AWS Security Hub Amazon Simple Storage Service, Amazon Detective o Amazon EventBridge, riducendo il livello di rumore delle ricerche se si utilizzano GuardDuty i risultati tramite Security Hub, un SIEM di terze parti o altre applicazioni di avviso e ticketing. Se l'hai abilitatoGuardDuty Protezione da malware, i GuardDuty risultati soppressi non avvieranno una scansione antimalware.

GuardDuty continua a generare risultati anche quando corrispondono alle regole di soppressione impostate, tuttavia tali risultati vengono automaticamente contrassegnati come archiviati. I risultati archiviati vengono archiviati GuardDuty per 90 giorni e possono essere visualizzati in qualsiasi momento durante tale periodo. Puoi visualizzare i risultati soppressi nella GuardDuty console selezionando Archiviato dalla tabella dei risultati o tramite l' GuardDuty API utilizzando l'ListFindingsAPI con un `findingCriteria` criterio uguale a true. `service.archived`

> **Note**
>
> In un ambiente con più account solo l' GuardDuty amministratore può creare regole di soppressione.

Casi d'uso comuni per le regole di eliminazione ed esempi

I seguenti tipi di esiti presentano casi d'uso comuni per l'applicazione delle regole di eliminazione. Seleziona il nome dell'esito per accedere a ulteriori dettagli sull'esito in questione o esamina le informazioni per creare una regola di eliminazione per questo tipo di esito dalla console.

> **Important**
>
> GuardDuty consiglia di creare regole di soppressione in modo reattivo e solo per i risultati per i quali sono stati ripetutamente identificati falsi positivi.

- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS: utilizza una regola di eliminazione per archiviare automaticamente gli esiti generati quando la rete VPC è configurata per instradare il traffico Internet in modo tale che esso esca da un gateway on-premise anziché da un gateway Internet VPC.

  Questo esito viene generato quando la rete è configurata per instradare il traffico Internet in modo tale da uscire da un gateway on-premise anziché da un gateway Internet (IGW) VPC. Configurazioni comuni, come l'utilizzo di AWS Outposts o delle connessioni VPN del VPC, possono instradare il traffico in questo modo. Se questo comportamento è previsto, si consiglia di utilizzare le regole di soppressione in e di creare una regola composta da due criteri di filtro. Il primo criterio è trovare il tipo, che dovrebbe essere `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. Il secondo criterio di filtro è l'Indirizzo IPv4 del chiamante API con l'indirizzo IP o l'intervallo CIDR del gateway Internet on-premise. L'esempio seguente rappresenta il filtro da utilizzare per eliminare questo tipo di esito in base all'indirizzo IP del chiamante API.

  ```
  Finding type: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
   API caller IPv4 address: 198.51.100.6
  ```

  > **Note**
  >
  > Per includere più IP del chiamante API, puoi aggiungere un nuovo filtro di Indirizzo IPv4 del chiamante API per ciascuno.

- Recon:EC2/Portscan: utilizza una regola di eliminazione per archiviare automaticamente gli esiti quando utilizzi un'applicazione di valutazione della vulnerabilità.

  La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `Recon:EC2/Portscan`. Il secondo criterio di filtro dovrebbe corrispondere all'istanza o alle istanze che ospitano questi strumenti di valutazione della vulnerabilità. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda dei criteri identificabili con le istanze che ospitano questi strumenti. L'esempio seguente rappresenta il filtro da utilizzare per eliminare questo tipo di esito in base a istanze con determinate AMI.

  ```
  Finding type: Recon:EC2/Portscan Instance image ID: ami-999999999
  ```

- UnauthorizedAccess:EC2/SSHBruteForce: utilizza una regola di eliminazione per archiviare automaticamente gli esiti quando è destinata a istanze di host bastione.

  Se l'obiettivo del tentativo di forza bruta è un bastion host, ciò può rappresentare il comportamento previsto per l'ambiente in uso. AWS In questo caso, si consiglia di impostare una regola di eliminazione per questa individuazione. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `UnauthorizedAccess:EC2/SSHBruteForce`. Il secondo criterio di filtro deve corrispondere all'istanza o alle istanze che fungono da bastion host. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda del criterio identificabile con le istanze che ospitano questi strumenti. L'esempio seguente rappresenta il filtro da utilizzare per eliminare questo tipo di esito in base a istanze con un determinato valore del tag dell'istanza.

  ```
  Finding type: UnauthorizedAccess:EC2/SSHBruteForce Instance tag value: devops
  ```

- Recon:EC2/PortProbeUnprotectedPort: utilizza una regola di eliminazione per archiviare automaticamente gli esiti quando è destinata a istanze esposte intenzionalmente.

  Tuttavia, ci possono essere casi in cui le istanze sono intenzionalmente esposte, ad esempio se ospitano server web. Se questo è il caso nel tuo AWS ambiente, ti consigliamo di impostare una regola di soppressione per questo risultato. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `Recon:EC2/PortProbeUnprotectedPort`. Il secondo criterio di filtro deve corrispondere all'istanza o alle istanze che fungono da bastion host. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda del criterio identificabile con le istanze che ospitano questi strumenti. L'esempio seguente rappresenta il filtro da utilizzare per eliminare questo tipo di esito in base a istanze con una determinata chiave di tag dell'istanza nella console.

  ```
  Finding type: Recon:EC2/PortProbeUnprotectedPort Instance tag key: prod
  ```

Regole di eliminazione consigliate per gli esiti del monitoraggio del runtime EKS

- PrivilegeEscalation:Runtime/DockerSocketAccessed viene generato quando un processo all'interno di un container comunica con il socket Docker. Nel tuo ambiente potrebbero esserci container che devono accedere al socket Docker per motivi legittimi. L'accesso da parte di tali container genererà esiti PrivilegeEscalation:Runtime/DockerSocketAccessed. Se questo è un caso nel tuo AWS ambiente, ti consigliamo di impostare una regola di soppressione per questo

tipo di risultato. Il primo criterio dovrebbe utilizzare il campo Tipo di risultato con valore uguale a `PrivilegeEscalation:Runtime/DockerSocketAccessed`. Il secondo criterio di filtro è il campo Percorso eseguibile con valore uguale al `executablePath` del processo nell'esito generato. In alternativa, il secondo criterio di filtro può utilizzare il campo SHA-256 eseguibile con valore uguale al `executableSha256` del processo nell'esito generato.

- I cluster Kubernetes gestiscono i propri server DNS come pod, ad esempio. `coredns` Pertanto, per ogni ricerca DNS da un pod, GuardDuty acquisisce due eventi DNS, uno dal pod e l'altro dal pod del server. Ciò può generare duplicati per i seguenti esiti DNS:
  - 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

  Gli esiti duplicati includeranno i dettagli del pod, del container e del processo che corrispondono al pod del server DNS. Puoi impostare una regola di eliminazione per eliminare gli esiti duplicati utilizzando questi campi. Il primo criterio di filtro deve utilizzare il campo Tipo di risultato con valore uguale a un tipo di esito DNS dall'elenco degli esiti fornito in precedenza in questa sezione. Il secondo criterio di filtro può essere Percorso eseguibile con valore uguale a quello del `executablePath` del server DNS o SHA-256 eseguibile con valore uguale a quello del `executableSHA256` del server DNS nell'esito generato. Come terzo criterio di filtro facoltativo, puoi utilizzare il campo Immagine del container di Kubernetes con valore uguale all'immagine del container del pod del server DNS nell'esito generato.

Per creare regole di soppressione in GuardDuty

Scegliete il metodo di accesso preferito per creare o gestire le regole di soppressione. GuardDuty

Console

È possibile visualizzare, creare e gestire le regole di soppressione utilizzando la console. GuardDuty Le regole di eliminazione vengono generate nello stesso modo dei filtri e i filtri esistenti salvati possono essere utilizzati come regole di eliminazione. Per ulteriori informazioni sulla creazione dei filtri, consulta Filtro dei risultati.

Per creare una regola di eliminazione utilizzando la console:

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nella pagina Risultati, scegli Elimina risultati per aprire il pannello delle regole di eliminazione.
3. Per aprire il menu dei criteri di filtro, inserisci i **`filter criteria`** in Aggiungi criteri filtro. Puoi scegliere un criterio dall'elenco. Inserisci un valore valido per il criterio scelto.

   > **Note**
   >
   > Per determinare quale sia il valore valido, visualizza la tabella degli esiti e scegli un esito da eliminare. Esaminane i dettagli nel pannello degli esiti.

   Puoi aggiungere più criteri di filtro e assicurarti che nella tabella compaiano solo gli esiti che desideri eliminare.
4. Inserisci un Nome e una Descrizione per la regola di eliminazione. I caratteri validi includono i caratteri alfanumerici, il punto (.), il trattino (-), il carattere di sottolineatura (_) e gli spazi bianchi.
5. Selezionare Salva.

Puoi anche creare una regola di eliminazione da un filtro esistente salvato. Per ulteriori informazioni sulla creazione dei filtri, consulta Filtro dei risultati.

Per creare una regola di eliminazione da un filtro salvato:

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nella pagina Risultati, scegli Elimina risultati per aprire il pannello delle regole di eliminazione.
3. Dal menu a discesa Regole salvate, scegli un filtro salvato.
4. Puoi anche aggiungere nuovi criteri di filtro. Salta questo passaggio se non sono necessari criteri di filtro aggiuntivi.

Per aprire il menu dei criteri di filtro, inserisci i **`filter criteria`** in Aggiungi criteri filtro. Puoi scegliere un criterio dall'elenco. Inserisci un valore valido per il criterio scelto.

> **Note**
>
> Per determinare quale sia il valore valido, visualizza la tabella degli esiti e scegli un esito da eliminare. Esaminane i dettagli nel pannello degli esiti.

5. Inserisci un Nome e una Descrizione per la regola di eliminazione. I caratteri validi includono i caratteri alfanumerici, il punto (.), il trattino (-), il carattere di sottolineatura (_) e gli spazi bianchi.
6. Selezionare Salva.

Per eliminare una regola di eliminazione:

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nella pagina Risultati, scegli Elimina risultati per aprire il pannello delle regole di eliminazione.
3. Dal menu a discesa Regole salvate, scegli un filtro salvato.
4. Scegliere Delete rule (Elimina regola).

API/CLI

Per creare una regola di eliminazione tramite API:

1. Puoi creare regole di eliminazione tramite l'API CreateFilter. Per farlo, specifica i criteri di filtro in un file JSON seguendo il formato dell'esempio riportato di seguito. L'esempio seguente eliminerà tutti gli esiti di gravità bassa non archiviati che presentano una richiesta DNS al dominio test.example.com. Per gli esiti di gravità media, l'elenco di input sarà `["4", "5", "7"]`, mentre per quelli di gravità alta, l'elenco di input sarà `["6", "7", "8"]`. Puoi anche applicare filtri in base a qualsiasi valore dell'elenco.

```
{
    "Criterion": {
        "service.archived": {
            "Eq": [
                "false"
            ]
```

```
        },
        "service.action.dnsRequestAction.domain": {
            "Eq": [
                "test.example.com"
            ]
        },
        "severity": {
            "Eq": [
                "1",
                "2",
                "3"
            ]
        }
    }
}
```

Per un elenco dei nomi dei campi JSON e il relativo equivalente della console, vedere Attributi del filtro.

Per testare i criteri di filtro, utilizza lo stesso criterio JSON nell'API ListFindings e conferma che siano stati selezionati gli esiti corretti. Per testare i criteri di filtro, AWS CLI segui l'esempio utilizzando il tuo detectorID e.json.

Per trovare i dati relativi al `detectorId` tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
aws guardduty list-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
finding-criteria file://criteria.json
```

2. Carica il filtro da utilizzare come regola di eliminazione con l'API CreateFilter o utilizzando la CLI AWS seguendo l'esempio riportato di seguito con il tuo ID rilevatore, un nome per la regola di eliminazione e il file.json.

   Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
aws guardduty create-filter --action ARCHIVE --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name yourfiltername --finding-criteria
 file://criteria.json
```

Puoi visualizzare un elenco dei tuoi filtri in modo programmatico con l'API ListFilter. Puoi visualizzare i dettagli di un singolo filtro fornendo il nome del filtro all'API GetFilter. Aggiorna i filtri utilizzando UpdateFilter o eliminali con l'API DeleteFilter.

Utilizzo di elenchi di indirizzi IP affidabili ed elenchi minacce

Amazon GuardDuty monitora la sicurezza del tuo AWS ambiente analizzando ed elaborando i log di flusso VPC, i log degli AWS CloudTrail eventi e i log DNS. Puoi personalizzare questo ambito di monitoraggio configurando GuardDuty in modo da bloccare gli avvisi per gli IP affidabili presenti nei tuoi elenchi di IP affidabili e avvisare gli IP dannosi noti presenti nei tuoi elenchi di minacce.

Gli elenchi di indirizzi IP affidabili e gli elenchi minacce si applicano solo al traffico destinato a indirizzi IP instradabili pubblicamente. Gli effetti di un elenco si applicano a tutti i log di flusso e ai CloudTrail risultati VPC, ma non si applicano ai risultati DNS.

GuardDuty può essere configurato per utilizzare i seguenti tipi di elenchi.

Elenco di indirizzi IP affidabili

Gli elenchi di IP affidabili sono costituiti da indirizzi IP attendibili per comunicazioni sicure con AWS l'infrastruttura e le applicazioni. GuardDuty non genera log di flusso VPC o CloudTrail risultati per gli indirizzi IP negli elenchi di IP affidabili. Puoi includere un massimo di 2.000 indirizzi IP e intervalli CIDR in un singolo elenco di IP affidabili. In qualsiasi momento, puoi avere soltanto un elenco di indirizzi IP affidabili caricato per account AWS per regione.

Elenco di IP delle minacce

Un elenco minacce è costituito dagli indirizzi IP dannosi noti. Questo elenco può essere fornito dall'intelligence sulle minacce di terze parti o creato appositamente per l'organizzazione. Oltre a generare risultati a causa di un'attività potenzialmente sospetta, genera GuardDuty anche risultati basati su questi elenchi di minacce. È possibile includere un massimo di 250.000 indirizzi IP e intervalli CIDR in un unico elenco di minacce. GuardDuty genera risultati solo sulla base di un'attività che coinvolge indirizzi IP e intervalli CIDR negli elenchi di minacce; i risultati non vengono generati in base ai nomi di dominio. In qualsiasi momento, puoi caricare fino a sei elenchi di minacce Account AWS per ogni regione.

> **Note**
>
> Se includi lo stesso IP sia in un elenco di IP affidabili che in un elenco minacce, l'IP verrà elaborato prima dall'elenco di indirizzi IP affidabili e non verrà generato alcun esito.

In ambienti con più account, solo gli utenti con account di GuardDuty amministratore possono aggiungere e gestire elenchi di IP affidabili ed elenchi di minacce. Gli elenchi di IP affidabili e gli elenchi di minacce caricati dall'account amministratore non possono funzionare GuardDuty correttamente negli account dei membri. In altre parole, negli account dei membri GuardDuty genera risultati basati su attività che coinvolgono indirizzi IP dannosi noti presenti negli elenchi di minacce dell'account amministratore e non genera risultati basati su attività che coinvolgono gli indirizzi IP degli elenchi di IP affidabili dell'account amministratore. Per ulteriori informazioni, consulta Gestione di più account in Amazon GuardDuty.

Formati di elenco

GuardDuty accetta elenchi nei seguenti formati.

La dimensione massima di ogni file che ospita l'elenco di indirizzi IP affidabili o di IP delle minacce è 35 MB. Nel tuo elenco degli indirizzi IP affidabili e di IP delle minacce, gli indirizzi IP e gli intervalli CIDR devono comparire uno per riga. Sono accettati solo indirizzi IPv4.

- Testo normale (TXT)

  Questo formato supporta sia blocchi CIDR che indirizzi IP individuali. Il seguente elenco di esempio utilizza il formato di testo normale (TXT).

  ```
  192.0.2.0/24
  198.51.100.1
  203.0.113.1
  ```

- Structured Threat Information Expression (STIX)

  Questo formato supporta sia blocchi CIDR che indirizzi IP individuali. Il seguente elenco di esempio utilizza il formato STIX.

  ```
  <?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>
```

- Open Threat Exchange (OTX)™ CSV

  Questo formato supporta sia blocchi CIDR che indirizzi IP individuali. Il seguente elenco di esempio utilizza il formato 0TX™ CSV.

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

- FireEye™ iSight Threat Intelligence CSV

  Questo formato supporta sia blocchi CIDR che indirizzi IP individuali. Il seguente elenco di esempio utilizza un formato `FireEye`™ CSV.

```
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
```

- Proofpoint™ ET Intelligence Feed CSV

  Questo formato supporta solo indirizzi IP individuali. Il seguente elenco di esempio utilizza il formato `Proofpoint` CSV. Il parametro `ports` è facoltativo. Se non inserisci il parametro porta, assicurati di lasciare una virgola finale (,).

```
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
```

- AlienVault Feed di reputazione™

  Questo formato supporta solo indirizzi IP individuali. Il seguente elenco di esempio utilizza il formato `AlienVault`.

```
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
```

Autorizzazioni necessarie per caricare elenchi di indirizzi IP affidabili ed elenchi minacce

Diverse identità IAM richiedono autorizzazioni speciali per lavorare con elenchi di IP affidabili e elenchi di minacce. GuardDuty Un'identità con la policy gestita AmazonGuardDutyFullAccess collegata può rinominare e disattivare soltanto gli elenchi di indirizzi IP affidabili e gli elenchi minacce caricati.

Per concedere a varie identità l'accesso completo alla gestione degli elenchi di indirizzi IP affidabili e gli elenchi minacce (in aggiunta alla ridenominazione e alla disattivazione, sono inclusi anche

l'aggiunta, l'attivazione, l'eliminazione e l'aggiornamento della posizione o del nome degli elenchi), assicurati che le operazioni seguenti siano presenti nella policy di autorizzazioni collegata a un utente, gruppo o ruolo:

```
{
    "Effect": "Allow",
    "Action": [
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::555555555555:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

> **Important**
>
> Queste operazioni non sono incluse nella policy gestita `AmazonGuardDutyFullAccess`.

Utilizzo della crittografia lato server per elenchi di indirizzi IP affidabili ed elenchi minacce

GuardDuty supporta i seguenti tipi di crittografia per gli elenchi: SSE-AES256 e SSE-KMS. SSE-C non è supportato. Per ulteriori informazioni sui tipi di crittografia per S3, consulta Protezione dei dati con la crittografia lato server.

Se l'elenco è crittografato utilizzando la crittografia lato server SSE-KMS, è necessario concedere al ruolo collegato al GuardDuty servizio l'autorizzazione a decrittografare il file per attivare l'elenco. AWSServiceRoleForAmazonGuardDuty Aggiungi la seguente istruzione alla policy della chiave KMS e sostituisci l'ID account con il tuo:

```
{
    "Sid": "AllowGuardDutyServiceRole",
    "Effect": "Allow",
    "Principal": {
    "AWS": "arn:aws:iam::123456789123:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty"
    },
    "Action": "kms:Decrypt*",
    "Resource": "*"
```

```
}
```

Aggiunta e attivazione di un elenco di indirizzi IP affidabili o di IP delle minacce

Scegli uno dei seguenti metodi di accesso per aggiungere e attivare un elenco di indirizzi IP affidabili o di IP delle minacce.

Console

(Facoltativo) fase 1: recupero dell'URL della posizione dell'elenco

1. Apri la console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/.
2. Nel pannello di navigazione, scegli Bucket.
3. Scegli il nome del bucket Amazon S3 che contiene l'elenco specifico che vuoi aggiungere.
4. Scegli il nome dell'oggetto (elenco) per visualizzarne i dettagli.
5. Nella scheda Proprietà, copia l'URI S3 per questo oggetto.

Fase 2: aggiunta di un elenco di indirizzi IP affidabili o un elenco minacce

> **Important**
>
> Per impostazione predefinita, in qualsiasi momento, puoi avere un solo elenco di indirizzi IP affidabili e fino a sei elenchi minacce.

1. GuardDuty Apri la console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Elenchi.
3. Nella pagina List management (Gestione dell'elenco), scegliere Add a trusted IP list (Aggiungi un elenco di IP affidabili) o Add a threat list (Aggiungi un elenco minacce).
4. In base alla selezione effettuata, verrà visualizzata una finestra di dialogo. Procedi come segue:

    a. Per Nome elenco, inserisci un nome per l'elenco.

    Vincoli di denominazione degli elenchi: il nome dell'elenco può includere lettere minuscole, lettere maiuscole, numeri, trattino (-) e trattino basso (_).

b. Per Posizione, fornisci la posizione in cui hai caricato l'elenco. Se non hai ancora una posizione, consulta Step 1: Fetching location URL of your list.

   Formato dell'URL della posizione

   - 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. Selezionare la casella di controllo I agree (Accetto).

d. Scegliere Add list (Aggiungi elenco). Per impostazione predefinita, lo Stato dell'elenco aggiunto è Inattivo. Affinché l'elenco sia efficace, è necessario attivarlo.

Fase 3: attivazione di un elenco di indirizzi IP affidabili o di un elenco minacce

1. GuardDuty Apri la console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Elenchi.
3. Nella pagina Gestione dell'elenco, seleziona l'elenco che desideri attivare.
4. Scegli Operazioni, quindi Attiva. Potrebbero essere necessari fino a 15 minuti prima che l'elenco sia efficace.

API/CLI

Per elenchi di indirizzi IP affidabili

- Esegui CreateIPSet. Assicurati di fornire il `detectorId` dell'account membro per il quale desideri creare questo elenco di indirizzi IP affidabili.

  Vincoli di denominazione degli elenchi: il nome dell'elenco può includere lettere minuscole, lettere maiuscole, numeri, trattino (-) e trattino basso (_).

  - In alternativa, puoi farlo eseguendo il comando AWS Command Line Interface seguente. Assicurati di sostituire il `detector-id` con l'ID rilevatore dell'account membro per il quale aggiornerai l'elenco degli indirizzi IP affidabili.

```
aws guardduty create-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --format Plaintext --location https://
s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/DOC-EXAMPLE-SOURCE-FILE.format --
activate
```

Per gli elenchi minacce

- Esegui CreateThreatIntelSet. Assicurati di fornire il `detectorId` dell'account membro per il quale desideri creare questo elenco minacce.
  - In alternativa, puoi farlo eseguendo il comando AWS Command Line Interface seguente. Assicurati di fornire il `detectorId` dell'account membro per il quale desideri creare un elenco minacce.

```
aws guardduty create-threat-intel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --
format Plaintext --location https://s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/
DOC-EXAMPLE-SOURCE-FILE.format --activate
```

> **Note**
>
> Dopo aver attivato o aggiornato un elenco di IP, la sincronizzazione dell'elenco GuardDuty potrebbe richiedere fino a 15 minuti.

Aggiornamento di elenchi di indirizzi IP affidabili e di elenchi minacce

È possibile aggiornare il nome di un elenco o gli indirizzi IP aggiunti a un elenco che è già stato aggiunto e attivato. Se si aggiorna un elenco, è necessario riattivarlo GuardDuty per utilizzare la versione più recente dell'elenco.

Scegli uno dei metodi di accesso per aggiornare un elenco di IP affidabili o un elenco minacce.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Elenchi.

3. Nella pagina Gestione dell'elenco, seleziona il set di IP affidabili o un elenco minacce che desideri aggiornare.
4. Seleziona Azioni, quindi scegli Modifica.
5. Nella finestra di dialogo Aggiorna elenco, aggiorna le informazioni in base alle esigenze.

   Vincoli di denominazione degli elenchi: il nome dell'elenco può includere lettere minuscole, lettere maiuscole, numeri, trattino (-) e trattino basso (_).
6. Scegli la casella Accetto, quindi Aggiorna elenco. Il valore nella colonna Stato diventerà Inattivo.
7. Riattivazione dell'elenco aggiornato

   a. Nella pagina Gestione dell'elenco, seleziona l'elenco che desideri riattivare.

   b. Scegli Operazioni, quindi Attiva.

API/CLI

1. Esegui UpdateIPSet per aggiornare un elenco di indirizzi IP affidabili.
   - In alternativa, puoi eseguire il comando AWS CLI seguente per aggiornare un elenco di indirizzi IP affidabili. Assicurati di sostituire il `detector-id` con l'ID rilevatore dell'account membro per il quale aggiornerai l'elenco degli indirizzi IP affidabili.

     ```
     aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
      --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
     activate
     ```
2. Eseguire UpdateThreatIntelSet per aggiornare un elenco minacce
   - In alternativa, puoi eseguire il comando AWS CLI seguente per aggiornare un elenco minacce. Assicurati di sostituire il `detector-id` con l'ID rilevatore dell'account membro per il quale aggiornerai l'elenco minacce.

     ```
     aws guardduty update-threatintel-set --detector-
     id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
     intel-set-id d4b94fc952d6912b8f3060768example --activate
     ```

Disattivazione o eliminazione di un elenco di indirizzi IP affidabili o un elenco minacce

Scegli uno dei metodi di accesso per eliminare (utilizzando la console) o disattivare (utilizzando API/CLI) un elenco di indirizzi IP affidabili o un elenco minacce.

Console

1. GuardDuty Apri la console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Elenchi.
3. Nella pagina Gestione dell'elenco, seleziona l'elenco che desideri eliminare.
4. Scegli Azioni, quindi Elimina.
5. Conferma l'operazione e scegli Elimina. L'elenco specifico non sarà più disponibile nella tabella.

API/CLI

1. Per un elenco di indirizzi IP affidabili

   Esegui UpdateIPSet per aggiornare un elenco di indirizzi IP affidabili.

   - In alternativa, puoi eseguire il comando AWS CLI seguente per aggiornare un elenco di indirizzi IP affidabili. Assicurati di sostituire il `detector-id` con l'ID rilevatore dell'account membro per il quale aggiornerai l'elenco degli indirizzi IP affidabili.

     Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

     ```
     aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
      --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
     no-activate
     ```

2. Per un elenco minacce

   Eseguire UpdateThreatIntelSet per aggiornare un elenco minacce

   - In alternativa, puoi eseguire il comando AWS CLI seguente per aggiornare un elenco di indirizzi IP affidabili. Assicurati di sostituire il `detector-id` con l'ID rilevatore dell'account membro per il quale aggiornerai l'elenco minacce.

```
aws guardduty update-threatintel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
intel-set-id d4b94fc952d6912b8f3060768example --no-activate
```

Esportazione degli esiti

GuardDuty conserva i risultati generati per un periodo di 90 giorni. GuardDuty esporta i risultati attivi su Amazon EventBridge (EventBridge). Facoltativamente, puoi esportare i risultati generati in un bucket Amazon Simple Storage Service (Amazon S3). Questo ti aiuterà a tenere traccia dei dati storici delle attività potenzialmente sospette nel tuo account e a valutare se le misure correttive consigliate hanno avuto successo.

Tutti i nuovi risultati attivi GuardDuty generati vengono esportati automaticamente entro circa 5 minuti dalla generazione del risultato. È possibile impostare la frequenza con cui vengono esportati gli aggiornamenti dei risultati attivi. EventBridge La frequenza selezionata si applica all'esportazione di nuove occorrenze di risultati esistenti nel bucket S3 (se configurato) e in Detective (se integrato). EventBridge Per informazioni su come GuardDuty aggrega più occorrenze di risultati esistenti, consulta. GuardDuty ricerca dell'aggregazione

Quando configuri le impostazioni per esportare i risultati in un bucket Amazon S3, GuardDuty utilizza AWS Key Management Service (AWS KMS) per crittografare i dati dei risultati nel bucket S3. Ciò richiede l'aggiunta di autorizzazioni al bucket S3 e alla AWS KMS chiave in modo che GuardDuty possa utilizzarle per esportare i risultati nel tuo account.

Indice

- Considerazioni
- Fase 1 — Autorizzazioni necessarie per esportare i risultati
- Fase 2: allegare la policy alla chiave KMS
- Fase 3: Allegare la policy al bucket Amazon S3
- Fase 4 - Esportazione dei risultati in un bucket S3 (console)
- Passaggio 5: impostazione della frequenza per esportare i risultati attivi aggiornati

Considerazioni

Prima di procedere con i prerequisiti e i passaggi per esportare i risultati, considera i seguenti concetti chiave:

- Le impostazioni di esportazione sono regionali: è necessario configurare le opzioni di esportazione in ogni regione in cui si utilizza. GuardDuty
- Esportazione dei risultati in bucket Amazon S3 in Regioni AWS diverse aree geografiche GuardDuty : supporta le seguenti impostazioni di esportazione:
  - Il bucket o l'oggetto Amazon S3 e la AWS KMS chiave devono appartenere allo stesso. Regione AWS
  - Per i risultati generati in una regione commerciale, puoi scegliere di esportarli in un bucket S3 in qualsiasi regione commerciale. Tuttavia, non puoi esportare questi risultati in un bucket S3 in una regione opt-in.
  - Per i risultati generati in una regione opt-in, puoi scegliere di esportarli nella stessa regione opt-in in cui vengono generati o in qualsiasi regione commerciale. Tuttavia, non puoi esportare i risultati da una regione opt-in a un'altra regione opt-in.
- Autorizzazioni per esportare i risultati: per configurare le impostazioni per l'esportazione dei risultati attivi, il bucket S3 deve disporre delle autorizzazioni che consentano di caricare oggetti. GuardDuty È inoltre necessario disporre di una AWS KMS chiave che GuardDuty possa essere utilizzata per crittografare i risultati.
- I risultati archiviati non vengono esportati: il comportamento predefinito prevede che i risultati archiviati, incluse le nuove istanze di risultati soppressi, non vengano esportati.

  Per esportare un risultato archiviato, è necessario rimuoverlo dall'archiviazione. Questo cambierà lo stato in Attivo. In base alla frequenza di esportazione, il risultato verrà esportato nel bucket S3 configurato.
- GuardDuty l'account amministratore può esportare i risultati generati negli account membro associati: quando si configurano i risultati di esportazione in un account amministratore, anche tutti i risultati degli account membro associati generati nella stessa regione vengono esportati nella stessa posizione configurata per l'account amministratore. Per ulteriori informazioni, consulta Comprensione della relazione tra account GuardDuty amministratore e account membro.

Fase 1 — Autorizzazioni necessarie per esportare i risultati

Quando configuri le impostazioni per l'esportazione dei risultati, selezioni un bucket Amazon S3 in cui archiviare i risultati e AWS KMS una chiave da utilizzare per la crittografia dei dati. Oltre alle GuardDuty autorizzazioni per le azioni, devi disporre anche delle autorizzazioni per le seguenti azioni per configurare correttamente le impostazioni per esportare i risultati:

- s3: GetBucketLocation
- s3: PutObject

Fase 2: allegare la policy alla chiave KMS

GuardDuty crittografa i dati dei risultati nel bucket utilizzando. AWS Key Management Service Per configurare correttamente le impostazioni, devi prima GuardDuty autorizzare l'uso di una chiave KMS. Puoi concedere le autorizzazioni collegando la policy alla tua chiave KMS.

Quando utilizzi una chiave KMS di un altro account, devi applicare la politica delle chiavi accedendo al proprietario della Account AWS chiave. Quando configuri le impostazioni per esportare i risultati, avrai anche bisogno della chiave ARN dell'account che possiede la chiave.

Per modificare la politica delle chiavi KMS per GuardDuty crittografare i risultati esportati

1. Apri la AWS KMS console all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, usa il selettore della regione nell'angolo superiore destro della pagina.
3. Seleziona una chiave KMS esistente o esegui i passaggi per creare una nuova chiave nella Guida per gli AWS Key Management Service sviluppatori, che utilizzerai per crittografare i risultati esportati.

   > **Note**
   >
   > La Regione AWS chiave KMS e il bucket Amazon S3 devono coincidere.

   Puoi utilizzare lo stesso bucket S3 e la stessa key pair KMS per esportare i risultati da qualsiasi regione applicabile. Per ulteriori informazioni, consulta Esportazione dei Considerazioni risultati tra regioni.

4. Nella sezione Key policy (Policy chiave), scegli Edit (Modifica).

   Se è visualizzata la visualizzazione Passa alla politica, selezionala per visualizzare la Politica chiave, quindi scegli Modifica.

5. Copia il seguente blocco di policy nella tua policy chiave KMS per concedere l' GuardDuty autorizzazione all'uso della tua chiave.

```
{
    "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. Modifica la politica sostituendo i seguenti valori formattati in *rosso nell'esempio* di policy:

   1. Sostituisci l'*ARN della chiave KMS* con l'Amazon Resource Name (ARN) della chiave KMS. Per individuare l'ARN della chiave, consulta Finding the key ID and ARN nella Developer Guide.AWS Key Management Service
   2. Sostituisci *123456789012* con l' Account AWS ID che possiede l'account che esporta i risultati. GuardDuty
   3. Sostituisci *Region2* con il luogo in cui vengono generati i risultati. Regione AWS GuardDuty
   4. Sostituisci l'*SourceDetectorID* con quello `detectorID` dell' GuardDuty account nella regione specifica in cui sono stati generati i risultati.

      Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

> **Note**
>
> Se lo utilizzi GuardDuty in una regione con attivazione, sostituisci il valore per «Servizio» con l'endpoint regionale per quella regione. Ad esempio, se utilizzi GuardDuty nella regione Medio Oriente (Bahrein) (me-south-1), sostituiscilo con. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` Per informazioni sugli endpoint per ogni regione opt-in, consulta endpoint e quote. GuardDuty

7. Se hai aggiunto l'informativa prima dell'informativa finale, aggiungi una virgola prima di aggiungere questa dichiarazione. Assicurati che la sintassi JSON della tua politica delle chiavi KMS sia valida.

   Selezionare Salva.

8. (Facoltativo) Copia la chiave ARN su un blocco note per utilizzarla nei passaggi successivi.

Fase 3: Allegare la policy al bucket Amazon S3

Aggiungi le autorizzazioni al bucket Amazon S3 in cui esporterai i risultati in modo da poter caricare oggetti in GuardDuty questo bucket S3. Indipendentemente dall'utilizzo di un bucket Amazon S3 che appartiene al tuo account o a un altro Account AWS, devi aggiungere queste autorizzazioni.

Se in qualsiasi momento decidi di esportare i risultati in un altro bucket S3, per continuare a esportare i risultati, devi aggiungere le autorizzazioni a quel bucket S3 e configurare nuovamente le impostazioni dei risultati di esportazione.

Se non disponi già di un bucket Amazon S3 in cui esportare questi risultati, consulta Creating a bucket nella Amazon S3 User Guide.

Per allegare le autorizzazioni alla tua policy sui bucket S3

1. Esegui i passaggi indicati in Per creare o modificare una policy sui bucket nella Guida per l'utente di Amazon S3, finché non viene visualizzata la pagina Modifica policy del bucket.
2. La policy di esempio mostra come concedere GuardDuty l'autorizzazione all'esportazione dei risultati nel bucket Amazon S3. Se modifichi il percorso dopo aver configurato i risultati di esportazione, devi modificare la politica per concedere l'autorizzazione alla nuova posizione.

Copia la seguente politica di esempio e incollala nell'editor delle politiche Bucket.

Se hai aggiunto l'informativa prima dell'informativa finale, aggiungi una virgola prima di aggiungere questa dichiarazione. Assicurati che la sintassi JSON della tua politica delle chiavi KMS sia valida.

Esempio di politica del bucket S3

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGuardDutygetBucketLocation",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "Amazon S3 bucket ARN",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "AllowGuardDutyPutObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
```

```
                }
            }
        },
        {
            "Sid": "DenyUnencryptedUploadsThis is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "DenyIncorrectHeaderThis is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id": "KMS key ARN"
                }
            }
        },
        {
            "Sid": "DenyNon-HTTPS",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
```

```
}
```

3. Modifica la politica sostituendo i seguenti valori formattati in *rosso* nell'esempio della politica:

   1. Sostituisci l'*ARN del bucket Amazon S3* con l'Amazon Resource Name (ARN) del bucket Amazon S3. Puoi trovare il Bucket ARN nella pagina Modifica policy del bucket nella console https://console.aws.amazon.com/s3/.
   2. Sostituisci *123456789012* con l' Account AWS ID che possiede l'account che esporta i risultati. GuardDuty
   3. Sostituisci *Region2* con il luogo in cui vengono generati i risultati. Regione AWS GuardDuty
   4. Sostituisci l'*SourceDetectorID* con quello `detectorID` dell' GuardDuty account nella regione specifica in cui sono stati generati i risultati.

      Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.
   5. Sostituisci *[prefisso opzionale]* parte del valore segnaposto *ARN/ [prefisso opzionale] del bucket S3* con una posizione di cartella opzionale in cui esportare i risultati. Per ulteriori informazioni sull'uso dei prefissi, consulta Organizing objects using prefixes nella Amazon S3 User Guide.

      Se fornisci una posizione opzionale per la cartella che non esiste già, la GuardDuty creerà solo se l'account associato al bucket S3 è lo stesso dell'account che esporta i risultati. Quando esporti i risultati in un bucket S3 che appartiene a un altro account, la posizione della cartella deve già esistere.
   6. Sostituisci l'*ARN della chiave KMS* con l'Amazon Resource Name (ARN) della chiave KMS associata alla crittografia dei risultati esportati nel bucket S3. Per individuare l'ARN della chiave, consulta Finding the key ID and ARN nella Developer Guide.AWS Key Management Service

> **Note**
>
> Se lo utilizzi GuardDuty in una regione con attivazione, sostituisci il valore per il «Servizio» con l'endpoint regionale per quella regione. Ad esempio, se utilizzi GuardDuty nella regione Medio Oriente (Bahrein) (me-south-1), sostituiscilo con. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-`

south-1.amazonaws.com" Per informazioni sugli endpoint per ogni regione opt-in, consulta endpoint e quote. GuardDuty

4. Selezionare Salva.

Fase 4 - Esportazione dei risultati in un bucket S3 (console)

GuardDuty consente di esportare i risultati in un bucket esistente in un altro. Account AWS

Quando crei un nuovo bucket S3 o scegli un bucket esistente nel tuo account, puoi aggiungere un prefisso opzionale. Quando configuri i risultati dell'esportazione, GuardDuty crea una nuova cartella nel bucket S3 per i risultati. Il prefisso verrà aggiunto alla struttura di cartelle predefinita creata. GuardDuty Ad esempio, il formato del prefisso opzionale. `/AWSLogs/123456789012/GuardDuty/Region`

> **Important**
>
> La chiave KMS e il bucket S3 devono trovarsi nella stessa regione.

Prima di completare questi passaggi, assicurati di aver collegato le rispettive politiche alla tua chiave KMS e al bucket S3 esistente.

Per configurare i risultati delle esportazioni

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella pagina Impostazioni, in Opzioni di esportazione di Findings, per il bucket S3, scegli Configura ora (o Modifica, se necessario).
4. Per l'ARN del bucket S3, inserisci. **`bucket ARN`** Per trovare l'ARN del bucket, consulta Visualizzazione delle proprietà di un bucket S3 nella Amazon S3 User Guide. Nella scheda Autorizzazioni della pagina delle proprietà del bucket associato nella console https://console.aws.amazon.com/guardduty/.
5. Per l'ARN della chiave KMS, inserisci. **`key ARN`** Per individuare l'ARN della chiave, consulta Finding the key ID and ARN nella Developer Guide.AWS Key Management Service

6. Allega politiche

   - Esegui i passaggi per allegare la policy del bucket S3. Per ulteriori informazioni, consulta Fase 3: Allegare la policy al bucket Amazon S3.

   - Esegui i passaggi per allegare la policy delle chiavi KMS. Per ulteriori informazioni, consulta Fase 2: allegare la policy alla chiave KMS.

7. Seleziona Save (Salva.

Passaggio 5: impostazione della frequenza per esportare i risultati attivi aggiornati

Configura la frequenza di esportazione dei risultati attivi aggiornati in base al tuo ambiente. Per impostazione predefinita, i risultati aggiornati vengono esportati ogni 6 ore. Ciò significa che tutti i risultati aggiornati dopo l'esportazione più recente sono inclusi nella successiva esportazione. Se i risultati aggiornati vengono esportati ogni 6 ore e l'esportazione avviene alle 12:00, qualsiasi scoperta che si aggiorna dopo le 12:00 viene esportata alle 18:00.

Per impostare la frequenza

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Seleziona Impostazioni.
3. Nella sezione Opzioni di esportazione dei risultati, scegli Frequenza dei risultati aggiornati. Questo imposta la frequenza per l'esportazione dei risultati Active aggiornati sia EventBridge su Amazon S3 che su Amazon S3. Puoi scegliere tra le seguenti opzioni:

   - Update EventBridge e S3 ogni 15 minuti
   - Update EventBridge e S3 ogni 1 ora
   - Update CWE and S3 every 6 hours (Aggiorna CWE e S3 ogni 6 ore) (predefinito)

4. Scegli Save changes (Salva modifiche).

Creazione di risposte personalizzate ai GuardDuty risultati con Amazon CloudWatch Events

GuardDuty crea un evento per Amazon CloudWatch Events quando si verifica una modifica dei risultati. La ricerca di modifiche che creerà un CloudWatch evento include risultati appena generati o risultati appena aggregati. Gli eventi vengono emessi secondo il principio del massimo sforzo.

A ogni GuardDuty risultato viene assegnato un ID di ricerca. GuardDuty crea un CloudWatch evento per ogni risultato con un ID di ricerca univoco. Tutte le occorrenze successive di un esito esistente vengono aggregate all'esito originale. Per ulteriori informazioni, consulta GuardDuty ricerca dell'aggregazione.

> **Note**
>
> Se il tuo account è un amministratore GuardDuty delegato, gli CloudWatch eventi vengono pubblicati sul tuo account e sull'account membro in cui è stato generato il risultato.

Utilizzando CloudWatch events with GuardDuty, puoi automatizzare le attività per aiutarti a rispondere ai problemi di sicurezza rivelati dai GuardDuty risultati.

Per ricevere notifiche sui GuardDuty risultati basati sugli CloudWatch Eventi, devi creare una regola CloudWatch Events e un obiettivo per GuardDuty. Questa regola consente CloudWatch di inviare notifiche relative ai risultati GuardDuty generati alla destinazione specificata nella regola. Per ulteriori informazioni, consulta Creazione di una regola CloudWatch Events e di un target per GuardDuty (CLI).

Argomenti

- CloudWatch Frequenza di notifica degli eventi per GuardDuty
- CloudWatch formato di evento per GuardDuty
- Creazione di una regola CloudWatch Events per notificare GuardDuty i risultati (console)
- Creazione di una regola CloudWatch Events e di un target per GuardDuty (CLI)
- CloudWatch Eventi per ambienti GuardDuty con più account

CloudWatch Frequenza di notifica degli eventi per GuardDuty

Notifiche per gli esiti appena generati con un ID esito univoco

GuardDuty invia una notifica in base all' CloudWatch evento entro 5 minuti dal riscontro. Questo evento (e questa notifica) include inoltre tutte le occorrenze successive di tale risultato che avvengono nei 5 minuti successivi alla generazione del risultato con un ID univoco.

> **Note**
>
> Per impostazione predefinita, le notifiche per gli esiti appena generati vengono inviate ogni 5 minuti. Questa frequenza non può essere aggiornata.

Notifiche per occorrenze di esiti successive

Per impostazione predefinita, per ogni risultato con un ID di risultato univoco, GuardDuty aggrega tutte le occorrenze successive di un particolare tipo di risultato che si verificano entro intervalli di 6 ore in un unico evento. GuardDuty invia quindi una notifica su queste occorrenze successive in base a questo evento. Per impostazione predefinita, per le ricorrenze successive dei risultati esistenti, GuardDuty invia notifiche basate sugli CloudWatch eventi ogni 6 ore.

Solo un account amministratore può personalizzare la frequenza predefinita delle notifiche inviate relative alle CloudWatch successive rilevazioni di eventi. Gli utenti di account membri non possono personalizzare la frequenza. Il valore di frequenza impostato dall'account amministratore nel proprio account è imposto alla GuardDuty funzionalità di tutti gli account membri. Se un utente di un account amministratore imposta questo valore di frequenza su 1 ora, tutti gli account membro avranno anche la frequenza di 1 ora di ricezione delle notifiche relative ai successivi ritrovamenti. Per ulteriori informazioni, consulta Gestione di più account in Amazon GuardDuty.

> **Note**
>
> In qualità di account amministratore, puoi personalizzare la frequenza predefinita delle notifiche relative ai successivi ritrovamenti. I valori possibili sono 15 minuti, 1 ora o 6 ore (impostazione predefinita). Per ulteriori informazioni sull'impostazione della frequenza di queste notifiche, consulta Passaggio 5: impostazione della frequenza per esportare i risultati attivi aggiornati.

Monitoraggio dei GuardDuty risultati archiviati con Events CloudWatch

Per i risultati archiviati manualmente, le occorrenze iniziali e tutte le successive di questi risultati (generate dopo il completamento dell'archiviazione) vengono inviate a CloudWatch Events secondo la frequenza sopra descritta.

Per i risultati archiviati automaticamente, le occorrenze iniziali e tutte le successive di questi risultati (generate dopo il completamento dell'archiviazione) non vengono inviate agli Eventi. CloudWatch

CloudWatch formato di evento per GuardDuty

Il formato dell' CloudWatch evento per GuardDuty .

```
{
 "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}
}
```

> **Note**
>
> Il valore di dettaglio restituisce i dettagli JSON di un singolo esito come oggetto, invece di restituire il valore "esiti", che può supportare più esiti all'interno di un array.

Per un elenco completo di tutti i parametri inclusi in `GUARDDUTY_FINDING_JSON_OBJECT`, consulta GetFindings. Il parametro `id` visualizzato in `GUARDDUTY_FINDING_JSON_OBJECT` è l'ID risultato descritto precedentemente.

Creazione di una regola CloudWatch Events per notificare GuardDuty i risultati (console)

Puoi utilizzare CloudWatch Events with GuardDuty per impostare avvisi di ricerca automatici inviando eventi di GuardDuty ricerca a un hub di messaggistica per aumentare la visibilità dei GuardDuty risultati. Questo argomento mostra come inviare avvisi di risultati via e-mail, Slack o Amazon Chime configurando un argomento SNS e collegando tale argomento a CloudWatch una regola di evento Events.

Impostare un argomento Amazon SNS e un endpoint

Per iniziare, devi impostare innanzitutto un argomento in Amazon Simple Notification Service e aggiungere un endpoint. Per ulteriori informazioni, consulta Nozioni di base nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Questa procedura stabilisce dove inviare i dati di ricerca. GuardDuty L'argomento SNS può essere aggiunto a una regola CloudWatch Events Event durante o dopo la creazione della Regola di evento.

Email setup

Creazione di un argomento SNS

1. Accedi alla console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Selezionare Argomenti dal riquadro di navigazione e quindi Crea argomento.
3. Nella sezione Crea argomento, seleziona Standard. Inserisci quindi un Nome argomento, ad esempio **`GuardDuty_to_Email`**. Altri dettagli sono facoltativi.
4. Seleziona Create Topic (Crea argomento). Verranno aperti i dettagli dell'argomento per il nuovo argomento.
5. Nella sezione Sottoscrizioni, scegliere Crea sottoscrizione.
6. a. Dal menu Protocollo selezionare E-mail.
   b. Nel campo Endpoint, aggiungere l'indirizzo e-mail a cui si desidera ricevere le notifiche.

> **Note**
>
> Dopo averlo creato, ti verrà richiesto di confermare l'abbonamento tramite il tuo client e-mail.

c. Scegli Crea sottoscrizione

7. Controlla la presenza di un messaggio di abbonamento nella Posta in arrivo e scegli Conferma sottoscrizione

Slack setup

Creazione di un argomento SNS

1. Accedi alla console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Selezionare Argomenti dal riquadro di navigazione e quindi Crea argomento.
3. Nella sezione Crea argomento, seleziona Standard. Inserisci quindi un Nome argomento, ad esempio **`GuardDuty_to_Slack`**. Altri dettagli sono facoltativi. Scegli Crea argomento per finalizzare.

Configurazione di un client AWS Chatbot

1. Passa alla console AWS Chatbot
2. Dal pannello Client configurati, seleziona Configura nuovo client.
3. Scegli Slack e conferma con "Configura".

> **Note**
>
> Quando scegli Slack devi confermare le autorizzazioni per permettere a AWS Chatbot di accedere al tuo canale selezionando "consenti".

4. Seleziona Configura un nuovo canale per aprire il riquadro dei dettagli di configurazione.

   a. Inserisci un nome per il canale.

   b. Per il canale Slack, scegli il canale che desideri utilizzare. Per utilizzare il canale Slack privato con AWS Chatbot, scegli Canale privato.

   c. In Slack, copia l'ID del canale privato facendo clic con il pulsante destro del mouse sul nome del canale e selezionando Copia collegamento.

   d. Sulla Console di gestione AWS, nella finestra AWS Chatbot, incolla l'ID che hai copiato da Slack nel campo ID canale privato.

   e. In Autorizzazioni, scegli di creare un ruolo IAM utilizzando un modello, se non disponi già di un ruolo.

f. Per i Modelli di policy, scegli Autorizzazioni di notifica. Questo è il modello di policy IAM per AWS Chatbot. Fornisce le autorizzazioni di lettura ed elenco necessarie per CloudWatch allarmi, eventi e registri e per argomenti di Amazon SNS.

g. Scegli la regione in cui hai creato in precedenza l'argomento SNS, quindi seleziona l'argomento Amazon SNS che hai creato per inviare notifiche al canale Slack.

5. Selezionare Configura.

Chime setup

Creazione di un argomento SNS

1. Accedi alla console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Selezionare Argomenti dal riquadro di navigazione e quindi Crea argomento.
3. Nella sezione Crea argomento, seleziona Standard. Inserisci quindi un Nome argomento, ad esempio **`GuardDuty_to_Chime`**. Altri dettagli sono facoltativi. Scegli Crea argomento per finalizzare.

Configurazione di un client AWS Chatbot

1. Passa alla console AWS Chatbot
2. Dal pannello Client configurati, seleziona Configura nuovo client.
3. Scegli Chime e conferma con "Configura".
4. Dal riquadro Dettagli di configurazione, inserisci un nome per il canale.
5. In Chime, apri la chat room desiderata

   a. Seleziona l'icona a forma di ingranaggio nell'angolo in alto a destra e scegli Manage webhooks and bots (Gestisci webhook e bot).

   b. Seleziona Copia URL per copiare l'URL del webhook negli appunti.

6. Nella Console di gestione AWS, nella finestra AWS Chatbot, incolla l'URL che hai copiato nel campo URL webhook.
7. In Autorizzazioni, scegli di creare un ruolo IAM utilizzando un modello, se non disponi già di un ruolo.
8. Per i Modelli di policy, scegli Autorizzazioni di notifica. Questo è il modello di policy IAM per AWS Chatbot. Fornisce le autorizzazioni di lettura ed elenco necessarie per CloudWatch allarmi, eventi e registri e per argomenti di Amazon SNS.

9. Scegli la regione in cui hai creato in precedenza l'argomento SNS, quindi seleziona l'argomento Amazon SNS che hai creato per inviare notifiche alla room Chime.
10. Selezionare Configura.

Imposta un evento per i risultati CloudWatch GuardDuty

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Selezionare Regole nel riquadro di navigazione e quindi Crea regola.
3. Dal menu Service Name, scegli GuardDuty.
4. Dal menu Tipo di evento, scegli GuardDutyRicerca.
5. Accanto a Anteprima modello di eventi, selezionare Modifica.
6. Incollare il codice JSON riportato di seguito in Anteprima modello di eventi e scegliere Salva

```
{
  "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
    ]
  }
}
```

> **Note**
>
> Il codice di cui sopra avviserà per qualsiasi ricerca media o alta.

7. Nella sezione Destinazioni fare clic su Aggiungi destinazione.
8. Dal menu Seleziona destinazioni, scegliere Argomento SNS.
9. Per Seleziona argomento, selezionare il nome dell'argomento SNS creato nel passaggio 1.
10. Configura l'input per l'evento.

    - Se stai configurando le notifiche per Chime o Slack, vai alla fase 11, il tipo di input predefinito è Evento con corrispondenza.
    - Se stai configurando le notifiche per e-mail tramite SNS, segui i passaggi seguenti per personalizzare il messaggio inviato alla tua casella di posta:

    a. Espandere Configura input, quindi selezionare Trasformatore di input.

    b. Copiare il codice seguente e incollarlo nel campo Percorso di input.

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

    c. Copiare il codice seguente e incollarlo nel campo Modello di input per formattare l'e-mail.

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type
 <Finding_Type> in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id%3D<Finding_ID>"
```

11. Fare clic su Configura dettagli.
12. Nella pagina Configura dettagli della regola, immettere Nome e Descrizione per la regola, quindi scegliere Crea regola.

Creazione di una regola CloudWatch Events e di un target per GuardDuty (CLI)

La procedura seguente mostra come utilizzare AWS CLI i comandi per creare una regola CloudWatch Events e un target per GuardDuty. In particolare, la procedura mostra come creare una regola che CloudWatch consenta di inviare eventi per tutti i risultati che GuardDuty generano e aggiungono una AWS Lambda funzione come destinazione per la regola.

> **Note**
>
> Oltre alle funzioni Lambda, CloudWatch supporta GuardDuty i seguenti tipi di destinazione: istanze Amazon EC2, flussi Amazon Kinesis, AWS Step Functions attività Amazon ECS, macchine a stati, comandi e destinazioni integrate. `run`

Puoi anche creare una regola e un target per CloudWatch gli eventi tramite la console Events. GuardDuty CloudWatch Per ulteriori informazioni e passaggi dettagliati, consulta Creazione di una regola CloudWatch Events che si attiva in base a un evento. Nella sezione Event Source (Origine eventi), selezionare **`GuardDuty`** per Service name (Nome servizio) e **`GuardDuty Finding`** per Event Type (Tipo di evento).

Per creare una regola e un target

1. Per creare una regola che CloudWatch consenta di inviare eventi per tutti i risultati GuardDuty generati, esegui il seguente comando CloudWatch CLI.

   ```
   AWS events put-rule --name Test --event-pattern "{\"source\":
   [\"aws.guardduty\"]}"
   ```

   > **Important**
   >
   > Puoi personalizzare ulteriormente la regola in modo che indichi di CloudWatch inviare eventi solo per un sottoinsieme dei risultati generati GuardDuty. Questo sottoinsieme è basato sull'attributo o sugli attributi di risultato specificati nella regola. Ad esempio,

utilizzate il seguente comando CLI per creare una regola che CloudWatch consenta di inviare solo eventi per i GuardDuty risultati con la gravità di 5 o 8:

```
AWS events put-rule --name Test --event-pattern "{\"source\":
[\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"],
\"detail\":{\"severity\":[5,8]}}"
```

A tale scopo, è possibile utilizzare uno qualsiasi dei valori di proprietà disponibili in JSON per GuardDuty i risultati.

2. Per collegare una funzione Lambda come destinazione per la regola creata nel passaggio 1, esegui il seguente comando CLI CloudWatch .

   ```
   AWS events put-targets --rule Test --targets
   Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
   ```

   > **Note**
   >
   > Assicurati di sostituire <your_function>nel comando precedente con la tua effettiva funzione Lambda per gli GuardDuty eventi.

3. Per aggiungere le autorizzazioni necessarie per richiamare la destinazione, esegui il comando CLI di Lambda seguente.

   ```
   AWS lambda add-permission --function-name <your_function> --statement-
   id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
   ```

   > **Note**
   >
   > Assicurati di sostituire <your_function>nel comando precedente con la tua effettiva funzione Lambda per gli GuardDuty eventi.

> **Note**
>
> Nella procedura precedente, utilizziamo una funzione Lambda come obiettivo per la regola che attiva CloudWatch gli eventi. Puoi anche configurare altre AWS risorse come obiettivi per attivare CloudWatch gli eventi. Per ulteriori informazioni, consulta PutTargets.

CloudWatch Eventi per ambienti GuardDuty con più account

In qualità di GuardDuty amministratore, le regole relative agli CloudWatch eventi nel tuo account verranno attivate in base ai risultati applicabili degli account dei tuoi membri. Ciò significa che se imposti una notifica di ricerca tramite CloudWatch Eventi nel tuo account amministratore, come descritto nella sezione precedente, riceverai una notifica in merito ai risultati di alta e media gravità generati dai tuoi account membro oltre che dai tuoi.

Puoi identificare l'account membro da cui ha avuto origine la GuardDuty scoperta utilizzando il `accountId` campo dei dettagli JSON del risultato.

Per iniziare a scrivere una regola di evento personalizzata per un account membro specifico nel tuo ambiente nella console, crea una nuova regola e incolla il seguente modello nell'Anteprima modello di eventi, aggiungendo l'ID dell'account membro per cui desideri attivare l'evento.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

> **Note**
>
> Questo esempio si attiverà con il rilevamento di qualsiasi esito relativo all'ID account elencato. È possibile aggiungere più ID separati da una virgola seguendo la sintassi JSON.

Comprensione CloudWatch dei log e dei motivi per cui le risorse vengono ignorate durante la scansione di Malware Protection

GuardDuty Malware Protection pubblica gli eventi nel tuo gruppo di CloudWatch log Amazon /aws/guardduty/ malware-scan-events. Puoi monitorare lo stato e il risultato della scansione delle risorse interessate per ciascuno degli eventi relativi alla scansione malware. Alcune risorse Amazon EC2 e alcuni volumi Amazon EBS potrebbero essere stati ignorati durante la scansione della protezione da malware.

Controllo dei GuardDuty log in Malware CloudWatch Protection

Esistono tre tipi di eventi di scansione supportati nel gruppo di log malware-scan-events CloudWatch /aws/guardduty/.

Nome dell'evento di scansione della protezione da malware	Spiegazione
`EC2_SCAN_STARTED`	Creato quando una protezione GuardDuty antimalware avvia il processo di scansione antimalware, ad esempio quando si prepara a scattare un'istantanea di un volume EBS.
`EC2_SCAN_COMPLETED`	Creato al termine della scansione di GuardDuty Malware Protection per almeno uno dei volumi EBS della risorsa interessata. Questo evento include anche lo `snapshotId` appartenente al volume EBS scansionato. Al termine della scansione, il risultato sarà `CLEAN`, `THREATS_FOUND` o `NOT_SCANNED` .
`EC2_SCAN_SKIPPED`	Creato quando la scansione GuardDuty Malware Protection ignora tutti i volumi EBS della risorsa interessata. Per identificare il motivo per cui vengono ignorati, seleziona l'evento corrispondente e visualizza i dettagli. Per ulteriori informazioni sui motivi per cui le risorse vengono ignorate, consulta Motivi

Nome dell'evento di scansione della protezione da malware	Spiegazione
	per cui una risorsa viene ignorata durante la scansione malware di seguito.

> **Note**
>
> Se utilizzi unAWS Organizations, gli eventi di CloudWatch registro degli account dei membri in Organizations vengono pubblicati sia nell'account amministratore che nel gruppo di registro dell'account membro.

Scegli il metodo di accesso preferito per visualizzare e interrogare CloudWatch gli eventi.

Console

1. Accedi AWS Management Console e apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, in Log, scegli Gruppi di log. Scegli il gruppo di malware-scan-events log /aws/guardduty/ per visualizzare gli eventi di scansione per Malware Protection. GuardDuty

   Per eseguire una query, scegli Log Insights.

   Per informazioni sull'esecuzione di una query, consulta Analyzing log data with CloudWatch Logs Insights nella Amazon CloudWatch User Guide.
3. Scegli ID scansione per monitorare i dettagli della risorsa interessata e gli esiti relativi al malware. Ad esempio, puoi eseguire la seguente query per filtrare gli eventi di CloudWatch registro utilizzando. `scanId` Assicurati di utilizzare il tuo *`scan-id`* valido.

   ```
   fields @timestamp, @message, scanRequestDetails.scanId as scanId
   | filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
   | sort @timestamp asc
   ```

API/CLI

- Per lavorare con i gruppi di log, consulta la sezione Ricerca AWS CLI nelle voci di log utilizzando l'Amazon CloudWatch User Guide.

  Scegli il gruppo di malware-scan-events log /aws/guardduty/ per visualizzare gli eventi di scansione per Malware Protection. GuardDuty
- Per visualizzare e filtrare gli eventi di log, consulta GetLogEventse FilterLogEvents, rispettivamente, nell'Amazon CloudWatch API Reference.

GuardDuty Conservazione dei log di Malware Protection

Il periodo di conservazione dei log predefinito per il gruppo /aws/guardduty/ è di 90 giorni, dopodiché gli eventi di malware-scan-events registro vengono eliminati automaticamente. Per modificare la politica di conservazione dei log per il tuo gruppo di CloudWatch log, vedi Modificare la conservazione dei dati di log in Logs o. CloudWatch PutRetentionPolicy

Motivi per cui una risorsa viene ignorata durante la scansione malware

Negli eventi relativi alla scansione malware, alcune risorse EC2 e alcuni volumi EBS potrebbero essere stati ignorati durante il processo di scansione. La tabella seguente elenca i motivi per cui GuardDuty Malware Protection potrebbe non scansionare le risorse. Se applicabile, utilizza i passaggi proposti per risolvere questi problemi ed esegui la scansione di queste risorse la prossima volta che GuardDuty Malware Protection avvia una scansione antimalware. Gli altri problemi vengono utilizzati per informarti sul corso degli eventi e non possono essere risolti.

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
`RESOURCE_NOT_FOUND`	Il `resourceArn` fornito per avviare la scansione antimalware on demand non è stato trovato nel tuo ambiente AWS.	Convalida il `resourceArn` dell'istanza Amazon EC2 o del carico di lavoro di un container e riprova.	

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
`ACCOUNT_INELIGIBLE`	L'ID AWS dell'account da cui hai provato ad avviare una scansione antimalware su richiesta non è abilitato. GuardDuty	Verifica che GuardDuty sia abilitato per questo AWS account. Quando ne GuardDuty abiliti uno nuovoRegione AWS, la sincronizzazione potrebbe richiedere fino a 20 minuti.	

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
`UNSUPPORTED_KEY_ENCRYPTION`	GuardDuty Malware Protection supporta volumi non crittografati e crittografati con chiave gestita dal cliente. Non supporta la scansione di volumi EBS crittografati utilizzando la Crittografia di Amazon EBS. Attualmente, esiste una differenza regionale per cui questo motivo di salto non è applicabile. Per ulteriori informazioni su questi aspettiRegioni AWS, vedere. Disponibilità di funzionalità specifiche per ogni regione	Sostituisci la chiave di crittografia con una chiave gestita dal cliente. Per ulteriori informazioni sui tipi di crittografia GuardDuty supportati, vedereVolumi Amazon EBS supportati per la scansione di malware.	

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
`EXCLUDED_BY_SCAN_SETTINGS`	L'istanza EC2 o il volume EBS sono stati esclusi durante la scansione malware. Esistono due motivazioni possibili: il tag è stato aggiunto all'elenco di inclusione, ma la risorsa non è associata a questo tag, il tag è stato aggiunto all'elenco di esclusione e la risorsa è associata a questo tag oppure il tag `GuardDuty Excluded` è impostato su `true` per questa risorsa.	Aggiorna le opzioni di scansione o i tag associati alla tua risorsa Amazon EC2. Per ulteriori informazioni, consulta Opzioni di scansione con tag definiti dall'utente.	
`UNSUPPORTED_VOLUME_SIZE`	Il volume è superiore a 1024 GB.	Non utilizzabile.	
`NO_VOLUMES_ATTACHED`	GuardDuty Malware Protection ha rilevato l'istanza nel tuo account, ma nessun volume EBS è stato collegato a questa istanza per procedere con la scansione.	Non utilizzabile.	

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
UNABLE_TO_SCAN	Si tratta di un errore interno del servizio.	Non utilizzabile.	
SNAPSHOT_NOT_FOUND	Le istantanee create dai volumi EBS e condivise con l'account del servizio non sono state trovate e GuardDuty Malware Protection non ha potuto procedere con la scansione.	Verifica che CloudTrail le istantanee non siano state rimosse intenzionalmente.	
SNAPSHOT_QUOTA_REACHED	Hai raggiunto il volume massimo consentito per gli snapshot per ogni regione. Per questo motivo non è possibile né conservare né creare nuovi snapshot.	Puoi rimuovere gli snapshot meno recenti o richiedere un aumento della quota. Puoi visualizzare il limite predefinito per gli snapshot per ogni regione e scoprire come richiedere l'aumento della quota in Service Quotas nella Guida di riferimento generale di AWS.	

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
`MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED`	Più di 11 volumi EBS sono stati collegati a un'istanza EC2. GuardDuty Malware Protection ha analizzato i primi 11 volumi EBS, ottenuti ordinandoli alfabeticamente. `deviceName`	Non utilizzabile.	
`UNSUPPORTED_PRODUCT_CODE_TYPE`	GuardDuty non supporta la scansione delle istanze con as. `productCode` `marketplace` Per ulteriori informazioni, consulta AMI a pagamento nella Guida per l'utente di Amazon EC2 per le istanze Linux. Per informazioni su `productCode` , consulta ProductCode, nella Documentazione di riferimento delle API di Amazon EC2.	Non utilizzabile.	

Segnalazione di falsi positivi nella protezione da malware di GuardDuty

Le scansioni della protezione da malware di GuardDuty possono identificare come malevolo o dannoso un file innocuo nell'istanza Amazon EC2 o nel carico di lavoro di un container. Per migliorare la tua esperienza con la protezione da malware e il servizio GuardDuty, puoi segnalare risultati falsi positivi se ritieni che un file identificato come malevolo o dannoso durante una scansione in realtà non contenga malware.

Invio di un file falso positivo

1. Accedi alla console https://console.aws.amazon.com/guardduty/.
2. Se identifichi un probabile risultato falso positivo, contatta AWS Support per avviare il processo di invio del file falso positivo.
3. Scegli Scansioni malware.
4. Scegli una scansione per visualizzare l'ID esito.
5. Fornisci l'ID esito. Devi fornire anche l'hash SHA-256 del file per assicurarti che la protezione da malware di GuardDuty abbia ricevuto il file corretto.
6. Il team AWS Support ti fornirà un URL Amazon Simple Storage Service (S3) che potrai utilizzare per caricare il file e l'hash SHA-256. Informa il team AWS Support dopo aver caricato correttamente il file.

   > **Warning**
   >
   > Non fornire direttamente il file o l'hash SHA-256 a AWS Support. Carica il file e l'hash su Amazon S3 solo tramite l'URL fornito. Se non carichi il file e l'hash entro sette giorni dalla ricezione dell'URL, quest'ultimo non sarà più valido. Se l'URL non è più valido, dovrai contattare AWS Support per riceverne uno nuovo.

   GuardDuty conserva il file per un periodo non superiore a 30 giorni. I membri del team GuardDuty analizzeranno il contenuto dell'invio e agiranno di conseguenza per migliorare la tua esperienza con la protezione da malware e il servizio GuardDuty.

Risolvere i problemi di sicurezza scoperti da GuardDuty

Amazon GuardDuty genera risultati che indicano potenziali problemi di sicurezza. In questa versione di GuardDuty, i potenziali problemi di sicurezza indicano che un'istanza EC2 o un carico di lavoro del container sono compromessi oppure un insieme di credenziali compromesse nell'ambiente in uso. AWS Le sezioni seguenti descrivono le operazioni di correzione consigliate per questi scenari. Eventuali scenari di correzione alternativi verranno descritti nella voce del tipo di esito specifico. Puoi accedere alle informazioni complete su un tipo di esito selezionandolo dalla tabella relativa ai tipi di esiti attivi.

Indice

- Correzione di un'istanza Amazon EC2 potenzialmente compromessa
- Riparazione di un bucket S3 potenzialmente compromesso
- Riparazione di un cluster ECS potenzialmente compromesso
- Riparazione delle credenziali potenzialmente compromesse AWS
- Riparazione di un contenitore autonomo potenzialmente compromesso
- Correzione degli esiti del monitoraggio dei log di audit EKS
- Correzione dei risultati del Runtime Monitoring
- Ripristino di un database potenzialmente compromesso
- Correzione di una funzione Lambda potenzialmente compromessa

Correzione di un'istanza Amazon EC2 potenzialmente compromessa

Segui questi passaggi consigliati per correggere un'istanza EC2 potenzialmente compromessa nel tuo ambiente: AWS

1. Identifica l'istanza Amazon EC2 potenzialmente compromessa

   Ricerca malware nell'istanza potenzialmente compromessa e rimuovi quello rilevato. Puoi utilizzare la Scansione antimalware on demand per identificare un eventuale malware nell'istanza EC2 potenzialmente compromessa o verificare Marketplace AWS per capire se esistono prodotti di partner utili per identificare e rimuovere il malware.

2. Isolare l'istanza Amazon EC2 potenzialmente compromessa

   Se possibile, utilizza i seguenti passaggi per isolare l'istanza potenzialmente compromessa:

   1. Crea un gruppo di sicurezza Isolation dedicato.
   2. Crea un'unica regola `0.0.0.0/0 (0-65535)` per tutto il traffico nelle regole in uscita.

      Quando si applica questa regola, convertirà tutto il traffico in uscita esistente (e nuovo) in non tracciato, bloccando tutte le sessioni in uscita stabilite. Per ulteriori informazioni, consulta Connessioni non tracciate.
   3. Rimuovi tutte le associazioni correnti dei gruppi di sicurezza dall'istanza potenzialmente compromessa.
   4. Associa il gruppo di sicurezza Isolation a questa istanza.

      Dopo l'associazione, elimina la regola `0.0.0.0/0 (0-65535)` per tutto il traffico dalle regole in uscita del gruppo di sicurezza Isolation.
3. Identifica l'origine dell'attività sospetta

   Se viene rilevato un malware, in base al tipo di esito nel tuo account, identifica e interrompi l'attività potenzialmente non autorizzata sull'istanza EC2. Ciò potrebbe richiedere operazioni come la chiusura di tutte le porte aperte, la modifica delle policy di accesso e l'aggiornamento delle applicazioni per correggere le vulnerabilità.

   Se non sei in grado di identificare e fermare attività non autorizzate sulla tua istanza EC2 potenzialmente compromessa, ti consigliamo di terminare l'istanza EC2 compromessa e sostituirla con una nuova istanza, se necessario. Le risorse supplementari seguenti ti consentono di proteggere ulteriormente le istanze EC2:

   - Sezioni sulla sicurezza e sulle reti in Best practice per Amazon EC2
   - Gruppi di sicurezza Amazon EC2 per le istanze Linux e Gruppi di sicurezza Amazon EC2 per le istanze Windows
   - Sicurezza in Amazon EC2
   - Suggerimenti per la protezione dell'istanza EC2 (Linux)
   - AWS migliori pratiche di sicurezza
   - Incidenti relativi al dominio dell'infrastruttura su AWS
4. Sfoglia AWS re:Post

   AWS re:Post Consulta https://forums.aws.amazon.com/index.jspa per ulteriore assistenza.

5. Invia una richiesta di supporto tecnico

   Se sei abbonato a un pacchetto Premium Support, puoi inviare una richiesta di supporto tecnico.

Riparazione di un bucket S3 potenzialmente compromesso

Segui questi passaggi consigliati per correggere un bucket Amazon S3 potenzialmente compromesso nel tuo ambiente: AWS

1. Identifica la risorsa S3 potenzialmente compromessa.

   Un GuardDuty risultato per S3 elencherà il bucket S3 associato, il relativo Amazon Resource Name (ARN) e il suo proprietario nei dettagli del risultato.
2. Identifica l'origine dell'attività sospetta e la chiamata API utilizzata.

   La chiamata API utilizzata verrà elencata come `API` nei dettagli del risultato. L'origine sarà un principale IAM (un ruolo, un utente o un account IAM) e i dettagli identificativi verranno elencati nell'esito. A seconda del tipo di origine, saranno disponibili informazioni sull'indirizzo IP remoto o sul dominio di origine che servono per valutare se l'origine era autorizzata o meno. Se il risultato riguardava credenziali di un'istanza Amazon EC2, verranno inclusi anche i dettagli per quella risorsa.
3. Determina se l'origine della chiamata era autorizzata ad accedere alla risorsa identificata.

   Ad esempio, considera i quesiti seguenti:
   - Se è stato coinvolto un utente IAM, è possibile che le sue credenziali siano state potenzialmente compromesse? Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.
   - Se un'API è stata richiamata da un principale che non aveva mai invocato questo tipo di API in precedenza, l'origine in questione necessita delle autorizzazioni di accesso per questa operazione? Le autorizzazioni del bucket possono essere ulteriormente limitate?
   - Se l'accesso è stato visualizzato dal nome utente `ANONYMOUS_PRINCIPAL` con tipo di utente di `AWSAccount`, significa che il bucket è pubblico e vi è stato effettuato l'accesso. Questo bucket dovrebbe essere pubblico? In caso negativo, consulta i consigli di sicurezza riportati di seguito per trovare soluzioni alternative alla condivisione delle risorse S3.
   - Se l'accesso è avvenuto tramite una chiamata `PreflightRequest` riuscita visualizzata dal nome utente `ANONYMOUS_PRINCIPAL` con tipo di utente `AWSAccount`, significa che il bucket ha un set di policy di condivisione delle risorse multiorigine (CORS). Questo bucket dovrebbe avere

una policy CORS? In caso negativo, assicurati che il bucket non sia stato involontariamente reso pubblico e consulta i consigli di sicurezza riportati di seguito per trovare soluzioni alternative alla condivisione delle risorse S3. Per ulteriori informazioni su CORS, consulta Utilizzo delle funzionalità Cross-Origin Resource Sharing (CORS) nella Guida per l'utente di S3.

4. Determina se il bucket S3 contiene dati sensibili.

   Usa Amazon Macie per determinare se il bucket S3 contiene dati sensibili, come informazioni di identificazione personale (PII), dati finanziari o credenziali. Se il rilevamento automatico dei dati sensibili è abilitato per il tuo account Macie, esamina i dettagli del bucket S3 per comprendere meglio il contenuto del bucket S3. Se questa funzionalità è disabilitata per il tuo account Macie, ti consigliamo di attivarla per accelerare la valutazione. In alternativa, puoi creare ed eseguire un processo di rilevamento dei dati sensibili per ispezionare gli oggetti del bucket S3 alla ricerca di dati sensibili. Per ulteriori informazioni, consulta Rilevamento dei dati sensibili con Macie.

Se l'accesso era autorizzato, puoi ignorare l'esito. La console https://console.aws.amazon.com/guardduty/ consente di impostare regole per eliminare completamente i singoli esiti in modo che non vengano più visualizzati. Per ulteriori informazioni, consulta Regole di eliminazione.

Se ritieni che i tuoi dati S3 siano stati esposti o consultati da soggetti non autorizzati, consulta i seguenti consigli sulla sicurezza di S3 per rafforzare le autorizzazioni e limitare l'accesso. Le soluzioni di correzione appropriate dipenderanno dalle esigenze dell'ambiente specifico.

Consigli basati su esigenze specifiche di accesso ai bucket S3

L'elenco seguente fornisce consigli basati su esigenze specifiche di accesso ai bucket Amazon S3:

- Per limitare l'accesso pubblico all'uso dei dati S3 in modo centralizzato, S3 blocca l'accesso pubblico. Le impostazioni di blocco dell'accesso pubblico possono essere abilitate per punti di accesso, bucket e AWS account tramite quattro diverse impostazioni per controllare la granularità dell'accesso. Per ulteriori informazioni, consulta Impostazioni del blocco dell'accesso pubblico S3.
- AWS Le policy di accesso possono essere utilizzate per controllare in che modo gli utenti IAM possono accedere alle tue risorse o come accedere ai tuoi bucket. Per ulteriori informazioni, consulta Utilizzo delle policy di bucket e delle policy utente.

  Inoltre, puoi utilizzare gli endpoint del cloud privato virtuale (VPC) con policy del bucket S3 per limitare l'accesso a endpoint VPC specifici. Per ulteriori informazioni, consulta Policy di bucket di esempio per gli endpoint VPC per Amazon S3

- Per consentire temporaneamente l'accesso ai tuoi oggetti S3 a entità attendibili esterne al tuo account, puoi creare un URL prefirmato tramite S3. Questo accesso viene creato utilizzando le credenziali dell'account e, a seconda delle credenziali utilizzate, può durare da 6 ore a 7 giorni. Per ulteriori informazioni, consulta Generazione di URL prefirmati con S3.
- Per i casi d'uso che richiedono la condivisione di oggetti S3 tra diverse origini, puoi utilizzare i punti di accesso S3 per creare set di autorizzazioni che limitano l'accesso solo a quelli che si trovano all'interno della tua rete privata. Per ulteriori informazioni, consulta Gestione dell'accesso ai dati con i punti di accesso Amazon S3.
- Per concedere l'accesso sicuro alle tue risorse S3 ad altri AWS account puoi utilizzare una lista di controllo degli accessi (ACL), per maggiori informazioni consulta Managing S3 Access with ACL.

Per ulteriori informazioni sulle opzioni di sicurezza di S3, consulta le migliori pratiche di sicurezza di S3.

Riparazione di un cluster ECS potenzialmente compromesso

Segui questi passaggi consigliati per correggere un cluster Amazon ECS potenzialmente compromesso nel tuo ambiente: AWS

1. Identifica il cluster ECS potenzialmente compromesso.

   Il risultato GuardDuty Malware Protection for ECS fornisce i dettagli del cluster ECS nel pannello dei dettagli del risultato.
2. Valuta l'origine del malware

   Valuta se il malware rilevato era presente nell'immagine del container. Se nell'immagine era presente un malware, identifica tutte le altre attività in esecuzione che utilizzano questa immagine. Per informazioni sull'esecuzione delle attività, consulta. ListTasks
3. Isolare le attività potenzialmente interessate

   Isola le attività interessate negando tutto il traffico in entrata e in uscita dall'attività. Una regola di negazione totale del traffico può aiutarti a fermare un attacco già in corso, interrompendo tutte le connessioni all'attività.

Se l'accesso era autorizzato, puoi ignorare l'esito. La console https://console.aws.amazon.com/guardduty/ consente di impostare regole per eliminare completamente i singoli esiti in modo che non vengano più visualizzati. Per ulteriori informazioni, consulta Regole di eliminazione.

Riparazione delle credenziali potenzialmente compromesse AWS

Segui questi passaggi consigliati per correggere le credenziali potenzialmente compromesse nel tuo ambiente: AWS

1. Identifica l'entità IAM potenzialmente compromessa e la chiamata API utilizzata.

   La chiamata API utilizzata verrà elencata come `API` nei dettagli del risultato. L'entità IAM (un ruolo o un utente IAM) e le relative informazioni identificative verranno elencate nella sezione Risorse dei dettagli del risultato. Il tipo di entità IAM coinvolta può essere determinato dal campo Tipo utente, il nome dell'entità IAM sarà nel campo Nome utente . Il tipo di entità IAM coinvolta nel risultato può anche essere determinato dall'ID chiave di accesso utilizzato.

   Per le chiavi che iniziano con `AKIA`:

   Questo tipo di chiave è una credenziale gestita dal cliente a lungo termine associata a un utente IAM o Utente root dell'account AWS. Per informazioni sulla gestione delle chiavi di accesso per gli utenti IAM, consulta Gestione delle chiavi di accesso per gli utenti IAM.

   Per le chiavi che iniziano con `ASIA`:

   Questo tipo di chiave è una credenziale temporanea a breve termine generata da AWS Security Token Service. Queste chiavi esistono solo per un breve periodo e non possono essere visualizzate o gestite nella console di AWS gestione. I ruoli IAM utilizzeranno sempre AWS STS le credenziali, ma possono anche essere generate per gli utenti IAM, per ulteriori informazioni, AWS STS consulta IAM: Temporary security credentials.

   Se è stato utilizzato un ruolo, il campo Nome utente indicherà il nome del ruolo utilizzato. Puoi determinare in che modo è stata richiesta la chiave AWS CloudTrail esaminando l'`sessionIssuer`elemento della voce di CloudTrail registro, per maggiori informazioni consulta IAM e AWS STS information in. CloudTrail

2. Esaminare le autorizzazioni per l'entità IAM.

   Apri la console IAM. A seconda del tipo di entità utilizzata, scegli la scheda Utenti o Ruoli e individua l'entità interessata digitando il nome identificato nel campo di ricerca. Utilizzare le schede Autorizzazione e Access Advisor per esaminare le autorizzazioni effettive per tale entità.

3. Stabilire se le credenziali dell'entità IAM sono state utilizzate legittimamente.

   Contattare l'utente delle credenziali per stabilire se l'attività era intenzionale.

Ad esempio, determina se l'utente ha:

- Ha richiamato l'operazione API elencata nel risultato GuardDuty
- Chiamato l'operazione API all'ora indicata nel risultato GuardDuty
- Chiamato l'operazione API dall'indirizzo IP indicato nel risultato GuardDuty

Se questa attività è un uso legittimo delle AWS credenziali, puoi ignorare il GuardDuty risultato. La console https://console.aws.amazon.com/guardduty/ consente di impostare regole per eliminare completamente i singoli esiti in modo che non vengano più visualizzati. Per ulteriori informazioni, consulta Regole di eliminazione.

Se non riesci a confermare se questa attività è un uso legittimo, potrebbe essere il risultato di una compromissione di una particolare chiave di accesso, ovvero le credenziali di accesso dell'utente IAM o forse l'intera. Account AWSSe sospetti che le tue credenziali siano state compromesse, consulta le informazioni contenute nell'articolo Le mie credenziali Account AWS potrebbero essere compromesse per risolvere il problema.

Riparazione di un contenitore autonomo potenzialmente compromesso

1. Isolare il contenitore potenzialmente compromesso

   I seguenti passaggi ti aiuteranno a identificare il carico di lavoro dei container potenzialmente dannoso:

   - Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
   - Nella pagina Risultati, scegli il risultato corrispondente per visualizzare il pannello dei risultati.
   - Nel pannello degli esiti, nella sezione Risorsa interessata, puoi visualizzare l'ID e il nome del container.

   Isola questo container dagli altri carichi di lavoro del container.
2. Metti in pausa il container

   Sospendi tutti i processi nel container.

   Per informazioni sul congelamento del contenitore, consulta Mettere in pausa un contenitore.

   Arresta il container

Se la fase precedente ha esito negativo e il container non si ferma, arrestane il funzionamento. Se hai abilitato la Conservazione degli snapshot funzione, GuardDuty conserverà le istantanee dei tuoi volumi EBS che contengono malware.

Per informazioni sull'arresto del contenitore, consulta Stop a container.

3. Valuta la presenza di malware

   Valuta se nell'immagine del container è presente un malware.

Se l'accesso era autorizzato, puoi ignorare l'esito. La console https://console.aws.amazon.com/guardduty/ consente di impostare regole per eliminare completamente i singoli esiti in modo che non vengano più visualizzati. La GuardDuty console consente di impostare regole per eliminare completamente i singoli risultati in modo che non vengano più visualizzati. Per ulteriori informazioni, consulta Regole di eliminazione.

Correzione degli esiti del monitoraggio dei log di audit EKS

Amazon GuardDuty genera risultati che indicano potenziali problemi di sicurezza di Kubernetes quando EKS Audit Log Monitoring è abilitato per il tuo account. Per ulteriori informazioni, consulta Monitoraggio dei log di audit EKS. Le sezioni seguenti descrivono le operazioni di correzione consigliate per questi scenari. Le operazioni correttive sono descritte nella voce relativa al tipo di esito specifico. Puoi accedere alle informazioni complete su un tipo di esito selezionandolo dalla tabella relativa ai tipi di esiti attivi.

Se uno qualsiasi dei tipi di esiti del monitoraggio dei log di audit EKS è stato generato per un'attività prevista, puoi prendere in considerazione l'aggiunta di Regole di eliminazione per evitare di ricevere avvisi in futuro.

Diversi tipi di attacchi e problemi di configurazione possono innescare GuardDuty i risultati di Kubernetes. Questa guida ti aiuta a identificare le cause principali delle GuardDuty rilevazioni relative al cluster e delinea le linee guida appropriate per la correzione. Le seguenti sono le cause principali che hanno portato ai risultati di GuardDuty Kubernetes:

- Potenziali problemi di configurazione
- Riparare gli utenti Kubernetes potenzialmente compromessi
- Riparazione dei pod Kubernetes potenzialmente compromessi

- Riparazione dei nodi Kubernetes potenzialmente compromessi
- Riparazione delle immagini dei container potenzialmente compromesse

> **Note**
>
> Prima della versione 1.14 di Kubernetes, il `system:unauthenticated` gruppo era associato a e per impostazione predefinita. `system:discovery` `system:basic-user` ClusterRoles Ciò potrebbe consentire l'accesso non intenzionale a utenti anonimi. Gli aggiornamenti del cluster non revocano le autorizzazioni, quindi potrebbero essere ancora valide anche se hai aggiornato il cluster alla versione 1.14 o successiva. Ti consigliamo di disassociare queste autorizzazioni dal gruppo `system:unauthenticated`.
> Per ulteriori informazioni sulla rimozione di queste autorizzazioni, consulta le best practice di sicurezza per Amazon EKS nella Amazon EKS User Guide.

Potenziali problemi di configurazione

Se un esito indica un problema di configurazione, consulta la sezione sulla correzione di tale esito per indicazioni su come risolvere il problema. Per ulteriori informazioni, consulta i seguenti tipi di esiti che indicano problemi di configurazione:

- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/KubeflowDashboardExposed
- Qualsiasi scoperta che finisce con SuccessfulAnonymousAccess

Riparare gli utenti Kubernetes potenzialmente compromessi

Un GuardDuty risultato può indicare un utente Kubernetes compromesso quando un utente identificato nel risultato ha eseguito un'azione API inaspettata. Puoi identificare l'utente nella sezione Dettagli utente Kubernetes dei dettagli di un esito nella console o nei `resources.eksClusterDetails.kubernetesDetails.kubernetesUserDetails` del file JSON degli esiti. Questi dettagli utente includono `user name`, `uid` e i gruppi Kubernetes a cui appartiene l'utente.

Se l'utente accedeva al carico di lavoro utilizzando un'entità IAM, puoi utilizzare la sezione `Access Key details` per identificare i dettagli di un ruolo o di un utente IAM. Consulta i seguenti tipi di utente e le linee guida per la correzione.

> **Note**
>
> Puoi utilizzare Amazon Detective per esaminare ulteriormente il ruolo o l'utente IAM identificato nell'esito. Mentre visualizzi i dettagli del ritrovamento GuardDuty sulla console, scegli Investiga in Detective. Quindi seleziona AWS l'utente o il ruolo dagli elementi elencati per esaminarlo in Detective.

Amministratore Kubernetes integrato: l'utente predefinito assegnato da Amazon EKS all'identità IAM che ha creato il cluster. Questo tipo di utente è identificato dal nome utente `kubernetes-admin`.

Per revocare l'accesso a un amministratore Kubernetes integrato:

- Identifica il `userType` nella sezione `Access Key details`.
  - Se il `userType` è un Ruolo e il ruolo appartiene a un ruolo dell'istanza EC2:
    - Identifica l'istanza e segui le istruzioni riportate in Correzione di un'istanza Amazon EC2 potenzialmente compromessa.
  - Se il `userType` è un Utente o un Ruolo assunto da un utente:
    1. Ruota la chiave di accesso dell'utente.
    2. Ruota tutti i segreti a cui l'utente ha avuto accesso.
    3. Controlla le informazioni in Il mio AWS account potrebbe essere compromesso per ulteriori dettagli.

Utente autenticato OIDC: un utente a cui è stato concesso l'accesso tramite un provider OIDC. In genere un utente OIDC ha un indirizzo e-mail come nome utente. Puoi verificare se il cluster utilizza OIDC con il comando seguente: `aws eks list-identity-provider-configs --cluster-name` *`your-cluster-name`*

Per revocare l'accesso a un utente autenticato OIDC:

1. Ruota le credenziali dell'utente nel provider OIDC.
2. Ruota tutti i segreti a cui l'utente ha avuto accesso.

AWS-Auth ConfigMap defined user: un utente IAM a cui è stato concesso l'accesso tramite un -auth. AWSConfigMap Per maggiori informazioni, consulta Gestione di utenti o ruoli IAM per il cluster nella guida per l'utente &EKS. Puoi esaminarne le autorizzazioni utilizzando il comando seguente: `kubectl edit configmaps aws-auth --namespace kube-system`

Per revocare l'accesso di un utente: AWS ConfigMap

1. Utilizzate il seguente comando per aprire. ConfigMap

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. Identifica il ruolo o la voce utente nella sezione MapRoles o MapUsers con lo stesso nome utente riportato nella sezione dei dettagli utente di Kubernetes del tuo risultato. GuardDuty Consulta l'esempio seguente, in cui l'utente amministratore è stato identificato in un esito.

```
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. Rimuovi quell'utente da. ConfigMap Consulta l'esempio seguente, in cui l'utente amministratore è stato rimosso.

```
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. Se il `userType` è un Utente o un Ruolo assunto da un utente:
   a. Ruota la chiave di accesso dell'utente.
   b. Ruota tutti i segreti a cui l'utente ha avuto accesso.
   c. Controlla le informazioni in Il mio AWS account potrebbe essere compromesso per ulteriori dettagli.

Se l'esito non ha una sezione `resource.accessKeyDetails`, l'utente è un account di servizio Kubernetes.

Account di servizio: l'account di servizio fornisce un'identità per i pod e può essere identificato da un nome utente con il formato seguente: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Per revocare l'accesso a un account di servizio:

1. Ruota le credenziali dell'account di servizio.
2. Consulta le linee guida sulla compromissione dei pod nella sezione seguente.

Riparazione dei pod Kubernetes potenzialmente compromessi

Quando si GuardDuty specificano i dettagli di un pod o di una risorsa di carico di lavoro all'interno della `resource.kubernetesDetails.kubernetesWorkloadDetails` sezione, quel pod o risorsa del carico di lavoro è stato potenzialmente compromesso. Un GuardDuty risultato può indicare che un singolo pod è stato compromesso o che più pod sono stati compromessi a causa di una risorsa di livello superiore. Consulta i seguenti scenari di compromissione per indicazioni su come identificare il pod o i pod che sono stati compromessi.

Compromissione di pod singoli

Se il campo `type` all'interno della sezione `resource.kubernetesDetails.kubernetesWorkloadDetails` è pod, l'esito identifica un singolo pod. Il campo nome è il `name` del pod e il campo `namespace` è il relativo spazio del nome.

Per informazioni sull'identificazione del nodo di lavoro che esegue i pod, consulta Identificare i pod e il nodo di lavoro in questione.

Pod compromessi tramite una risorsa del carico di lavoro

Se il campo `type` all'interno della sezione `resource.kubernetesDetails.kubernetesWorkloadDetails` identifica una Risorsa del carico di lavoro, ad esempio un'`Deployment`, è probabile che tutti i pod all'interno della risorsa del carico di lavoro siano stati compromessi.

Per informazioni sull'identificazione di tutti i pod della risorsa del carico di lavoro e dei nodi su cui sono in esecuzione, consulta Identificare i pod e i nodi di lavoro pericolosi utilizzando il nome del carico di lavoro.

I pod sono stati compromessi tramite un account di servizio

Se un GuardDuty risultato identifica un account di servizio nella `resource.kubernetesDetails.kubernetesUserDetails` sezione, è probabile che i pod che utilizzano l'account di servizio identificato siano compromessi. Il nome utente riportato da un esito è un account di servizio se ha il formato seguente: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Per informazioni sull'identificazione di tutti i pod e i nodi di lavoro che utilizzano l'account di servizio e i nodi su cui sono in esecuzione, consulta Identificare i pod e i nodi di lavoro pericolosi utilizzando il nome dell'account di servizio.

Dopo aver identificato tutti i pod compromessi e i nodi su cui sono in esecuzione, consulta la guida alle best practice di Amazon EKS per isolare il pod, ruotarne le credenziali e raccogliere dati per l'analisi forense.

Per riparare un pod potenzialmente compromesso:

1. Identifica la vulnerabilità che ha compromesso i pod.
2. Implementa la correzione di tale vulnerabilità e avvia nuovi pod sostitutivi.

3. Eliminare i pod vulnerabili.

   Per ulteriori informazioni, consulta Ridistribuire il pod o la risorsa del carico di lavoro compromessa.

Se al nodo di lavoro è stato assegnato un ruolo IAM che consente ai Pods di accedere ad altre AWS risorse, rimuovi tali ruoli dall'istanza per evitare ulteriori danni causati dall'attacco. Allo stesso modo, se al pod è stato assegnato un ruolo IAM, valuta se puoi rimuovere in sicurezza le policy IAM dal ruolo senza influire sugli altri carichi di lavoro.

Riparazione delle immagini dei container potenzialmente compromesse

Quando un GuardDuty risultato indica una compromissione del pod, l'immagine utilizzata per avviare il pod potrebbe essere potenzialmente dannosa o compromessa. GuardDuty i risultati identificano l'immagine del contenitore all'interno del `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` campo. Puoi determinare se l'immagine è dannosa scansionandola alla ricerca di malware.

Per correggere un'immagine del contenitore potenzialmente compromessa:

1. Interrompi immediatamente l'utilizzo dell'immagine e rimuovila dal tuo repository di immagini.
2. Identifica tutti i pod utilizzando l'immagine potenzialmente compromessa.

   Per ulteriori informazioni, consulta Identificare i pod con immagini di container e nodi di lavoro potenzialmente vulnerabili o compromessi.
3. Isola i pod potenzialmente compromessi, ruota le credenziali e raccogli dati per l'analisi. Per ulteriori informazioni, consulta la guida alle best practice di Amazon EKS.
4. Elimina tutti i pod utilizzando l'immagine potenzialmente compromessa.

Riparazione dei nodi Kubernetes potenzialmente compromessi

Un GuardDuty risultato può indicare una compromissione del nodo se l'utente identificato nel risultato rappresenta l'identità di un nodo o se il risultato indica l'uso di un contenitore privilegiato.

L'identità utente è un nodo worker se il campo nome utente ha il seguente formato: `system:node:node name`. Ad esempio, `system:node:ip-192-168-3-201.ec2.internal`. Ciò indica che l'avversario ha ottenuto l'accesso al nodo e ne utilizza le credenziali per comunicare con l'endpoint dell'API Kubernetes.

Un esito indica l'uso di un container privilegiato se il campo `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.` dell'esito di uno o più container elencati nell'esito è impostato su `True`.

Per riparare un nodo potenzialmente compromesso:

1. Isola il pod, ruota le sue credenziali e raccogli dati per l'analisi forense.

   Per ulteriori informazioni, consulta la guida alle best practice di Amazon EKS.
2. Identifica gli account di servizio utilizzati da tutti i pod in esecuzione sul nodo potenzialmente compromesso. Controlla le relative autorizzazioni e, se necessario, ruota gli account di servizio.
3. Termina il nodo potenzialmente compromesso.

Correzione dei risultati del Runtime Monitoring

Quando abiliti il Runtime Monitoring per il tuo account, Amazon GuardDuty potrebbe generare dati Tipi di risultati del monitoraggio del runtime che indicano potenziali problemi di sicurezza nel tuo AWS ambiente. I potenziali problemi di sicurezza indicano un'istanza Amazon EC2 compromessa, un carico di lavoro del container, un cluster Amazon EKS o un set di credenziali compromesse nel tuo ambiente. AWS L'agente di sicurezza monitora gli eventi di runtime da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nei dettagli di ricerca generati nella GuardDuty console. La sezione seguente descrive le procedure di correzione consigliate per ogni tipo di risorsa.

Instance

Se il Tipo di risorsa nei dettagli dell'esito è Istanza, significa che un'istanza EC2 o un nodo EKS sono potenzialmente compromessi.

- Per correggere un nodo EKS compromesso, consulta Riparazione dei nodi Kubernetes potenzialmente compromessi.
- Per correggere un'istanza EC2 compromessa, consulta Correzione di un'istanza Amazon EC2 potenzialmente compromessa.

EKSCluster

Se il Tipo di risorsa nei dettagli dell'esito è EKSCluster, significa che un pod o un container in un cluster EKS sono potenzialmente compromessi.

- Per correggere un pod compromesso, consulta Riparazione dei pod Kubernetes potenzialmente compromessi.
- Per correggere l'immagine di un container compromessa, consulta Riparazione delle immagini dei container potenzialmente compromesse.

ECSCluster

Se il tipo di risorsa nei dettagli del risultato è ECSCluster, indica che un'attività ECS o un contenitore all'interno di un'attività ECS è potenzialmente compromessa.

1. Identifica il cluster ECS interessato

   Il risultato del GuardDuty Runtime Monitoring fornisce i dettagli del cluster ECS nel pannello dei dettagli del risultato o nella `resource.ecsClusterDetails` sezione del JSON di ricerca.

2. Identifica l'attività ECS interessata

   Il risultato GuardDuty di Runtime Monitoring fornisce i dettagli dell'attività ECS nel pannello dei dettagli del risultato o nella `resource.ecsClusterDetails.taskDetails` sezione del file JSON di ricerca.

3. Isola l'attività interessata

   Isola l'attività interessata bloccando tutto il traffico in entrata e in uscita verso l'attività. Una regola di blocco totale del traffico può contribuire a fermare un attacco già in corso, interrompendo tutte le connessioni all'attività.

4. Risolvi l'attività compromessa

   a. Identifica la vulnerabilità che ha compromesso l'attività.

   b. Implementa la correzione di tale vulnerabilità e riavvia l'attività sostitutiva.

   c. Interrompi l'attività vulnerabile.

Container

Se il Tipo di risorsa nei dettagli dell'esito è Container, significa che un container autonomo è potenzialmente compromesso.

- Per procedere alla correzione, consulta Riparazione di un contenitore autonomo potenzialmente compromesso.

- Se l'esito viene generato su più container utilizzando la stessa immagine del container, consulta Riparazione delle immagini dei container potenzialmente compromesse.
- Se il container ha avuto accesso all'host EC2 sottostante, le credenziali dell'istanza associata potrebbero essere state compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.
- Se un utente potenzialmente malintenzionato ha avuto accesso al nodo EKS sottostante o a un'istanza EC2, consulta la correzione consigliata nelle schede EKSCluster e Istanza.

Correzione delle immagini del container compromesse

Quando un GuardDuty risultato indica una compromissione dell'attività, l'immagine utilizzata per avviare l'attività potrebbe essere dannosa o compromessa. GuardDuty i risultati identificano l'immagine del contenitore all'interno del `resource.ecsClusterDetails.taskDetails.containers.image` campo. È possibile determinare se l'immagine è dannosa o meno eseguendo una scansione alla ricerca di malware.

Per correggere l'immagine compromessa di un contenitore

1. Interrompi immediatamente l'utilizzo dell'immagine e rimuovila dal tuo repository di immagini.
2. Identifica tutte le attività che utilizzano questa immagine.
3. Interrompi tutte le attività che utilizzano l'immagine compromessa. Aggiorna le definizioni delle attività in modo che smettano di utilizzare l'immagine compromessa.

Ripristino di un database potenzialmente compromesso

GuardDuty generi Tipi di esiti della Protezione RDS che indicano un comportamento di accesso potenzialmente sospetto e anomalo dopo l'attivazione. Database supportati GuardDuty Protezione RDS Utilizzando l'attività di accesso RDS, GuardDuty analizza e profila le minacce identificando modelli insoliti nei tentativi di accesso.

> **Note**
>
> Puoi accedere alle informazioni complete su un tipo di esito selezionandolo dalla Tabella degli esiti.

Segui questi passaggi consigliati per correggere un database Amazon Aurora potenzialmente compromesso nel tuo ambiente. AWS

Argomenti

- Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti
- Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti
- Correzione di credenziali potenzialmente compromesse
- Limita l'accesso alla rete

Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti

I seguenti passaggi consigliati sono utili per correggere un database Aurora potenzialmente compromesso che presenta un comportamento insolito legato a eventi di accesso riusciti.

1. Identifica il database e l'utente interessati.

   Il GuardDuty risultato generato fornisce il nome del database interessato e i dettagli utente corrispondenti. Per ulteriori informazioni, consulta Dettagli degli esiti.
2. Verifica se questo comportamento è previsto o non previsto.

   L'elenco seguente specifica i potenziali scenari che potrebbero aver causato la generazione GuardDuty di un risultato:
   - Un utente che accede al proprio database dopo un lungo periodo di tempo.
   - Un utente che accede occasionalmente al proprio database, ad esempio un analista finanziario che accede ogni tre mesi.
   - Un attore potenzialmente sospetto coinvolto in un tentativo di accesso riuscito può compromettere il database.
3. Inizia questa fase se il comportamento non è previsto.

   1. Limita l'accesso al database

      Limita l'accesso al database per gli account sospetti e per l'origine di questa attività di accesso. Per ulteriori informazioni, consultare Correzione di credenziali potenzialmente compromesse e Limita l'accesso alla rete.
   2. Valuta l'impatto e determina a quali informazioni è stato effettuato l'accesso.

- Se disponibili, esamina i log di audit per identificare le informazioni a cui potrebbe essere stato effettuato l'accesso. Per ulteriori informazioni, consulta Monitoraggio di eventi, registri e flussi in un cluster di database Amazon Aurora nella Guida per l'utente di Amazon Aurora.
- Determina se sono stati effettuati accessi o modifiche a informazioni sensibili o protette.

Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti

I seguenti passaggi consigliati sono utili per correggere un database Aurora potenzialmente compromesso che presenta un comportamento insolito legato a eventi di accesso falliti.

1. Identifica il database e l'utente interessati.

   Il GuardDuty risultato generato fornisce il nome del database interessato e i dettagli utente corrispondenti. Per ulteriori informazioni, consulta Dettagli degli esiti.
2. Identifica l'origine dei tentativi di accesso falliti.

   Il GuardDuty risultato generato fornisce l'indirizzo IP e l'organizzazione ASN (se si trattava di una connessione pubblica) nella sezione Attore del pannello di ricerca.

   Un sistema autonomo (AS) è un gruppo di uno o più prefissi IP (elenchi di indirizzi IP accessibili su una rete) gestiti da uno o più operatori di rete che mantengono un'unica policy di instradamento chiaramente definita. Gli operatori di rete necessitano di numeri di sistema autonomi (ASN) per controllare l'instradamento all'interno delle proprie reti e scambiare informazioni di instradamento con altri provider di servizi Internet (ISP).
3. Verifica che questo comportamento non sia previsto.

   Verifica nel modo seguente se questa attività rappresenta un tentativo di ottenere un ulteriore accesso non autorizzato al database:
   - Se l'origine è interna, verifica se un'applicazione non è configurata correttamente e tenta ripetutamente di stabilire una connessione.
   - Se si tratta di un attore esterno, verificate se il database corrispondente è pubblico o non correttamente configurato, permettendo così ai potenziali utenti malintenzionati di usare la forza bruta con nomi utente comuni.
4. Inizia questa fase se il comportamento non è previsto.

   1. Limita l'accesso al database

Limita l'accesso al database per gli account sospetti e per l'origine di questa attività di accesso. Per ulteriori informazioni, consultare Correzione di credenziali potenzialmente compromesse e Limita l'accesso alla rete.

2. Esegui l'analisi delle cause principali e determina i passaggi che potenzialmente hanno portato a questa attività.

   Imposta un avviso per ricevere una notifica quando un'attività modifica una policy di rete e crea uno stato di insicurezza. Per ulteriori informazioni, consulta Policy del firewall in AWS Network Firewall nella Guida per gli sviluppatori diAWS Network Firewall .

Correzione di credenziali potenzialmente compromesse

Un GuardDuty risultato può indicare che le credenziali dell'utente per un database interessato sono state compromesse quando l'utente identificato nel risultato ha eseguito un'operazione imprevista sul database. Puoi identificare l'utente nella sezione dei Dettagli utente del database RDS all'interno del pannello dell'esito nella console o all'interno dei `resource.rdsDbUserDetails` del file JSON degli esiti. Questi dettagli utente includono il nome utente, l'applicazione utilizzata, il database a cui si accede, la versione SSL e il metodo di autenticazione.

- Per revocare l'accesso o ruotare le password per utenti specifici coinvolti nell'esito, consulta Sicurezza con Amazon Aurora MySQL o Sicurezza con Amazon Aurora PostgreSQL nella Guida per l'utente di Amazon Aurora.
- Utilizzalo AWS Secrets Manager per archiviare in modo sicuro e ruotare automaticamente i segreti per i database Amazon Relational Database Service (RDS). Per ulteriori informazioni, consulta Tutorial diAWS Secrets Manager nella Guida per l'utente diAWS Secrets Manager .
- Utilizza l'autenticazione del database IAM per gestire l'accesso degli utenti del database senza bisogno di password. Per ulteriori informazioni, consulta Autenticazione database IAM nella Guida per l'utente di Amazon Aurora.

  Per ulteriori informazioni, consulta Best practice di sicurezza per Amazon Relational Database Service nella Guida per l'utente di Amazon RDS.

Limita l'accesso alla rete

Un GuardDuty risultato può indicare che un database è accessibile anche al di fuori delle applicazioni o del Virtual Private Cloud (VPC). Se l'indirizzo IP remoto indicato nell'esito è un'origine di

connessione non prevista, controlla i gruppi di sicurezza. Un elenco dei gruppi di sicurezza collegati al database è disponibile in Gruppi di sicurezza nella console https://console.aws.amazon.com/rds/ o nei `resource.rdsDbInstanceDetails.dbSecurityGroups` del file JSON degli esiti. Per maggiori informazioni sulla configurazione dei gruppi di sicurezza, consulta Controllo dell'accesso con i gruppi di sicurezza nella Guida dell'utente di Amazon RDS.

Se utilizzi un firewall, limita l'accesso alla rete al database riconfigurando le liste di controllo degli accessi di rete (NACL). Per ulteriori informazioni, consulta Firewall in AWS Network Firewall nella Guida per gli sviluppatori diAWS Network Firewall .

Correzione di una funzione Lambda potenzialmente compromessa

Quando GuardDuty genera un risultato di Lambda Protection e l'attività è inaspettata, la funzione Lambda potrebbe essere compromessa. Ti consigliamo di completare la procedura seguente per correggere una funzione Lambda compromessa.

Per correggere gli esiti della Protezione Lambda

1. Identifica la versione della funzione Lambda potenzialmente compromessa.

   Un GuardDuty risultato di Lambda Protection fornisce il nome, Amazon Resource Name (ARN), la versione della funzione e l'ID di revisione associati alla funzione Lambda elencati nei dettagli del risultato.
2. Identifica l'origine dell'attività potenzialmente sospetta.

   a. Esamina il codice associato alla versione della funzione Lambda coinvolta nell'esito.
   b. Esamina le librerie importate e i livelli della versione della funzione Lambda coinvolta nell'esito.
   c. Se hai abilitato AWS Lambda le funzioni di scansione con Amazon Inspector, esamina i risultati di Amazon Inspector associati alla funzione Lambda coinvolta nel risultato.
   d. AWS CloudTrail Esamina i log per identificare la causa principale che ha causato l'aggiornamento della funzione e assicurati che l'attività sia stata autorizzata o prevista.
3. Correggi la funzione Lambda potenzialmente compromessa.

   a. Disabilita i trigger di esecuzione della funzione Lambda coinvolta nell'esito. Per ulteriori informazioni, consulta. DeleteFunctionEventInvokeConfig
   b. Esamina il codice Lambda e aggiorna le importazioni delle librerie e i Livelli della funzione Lambda per rimuovere le librerie e i livelli potenzialmente sospetti.

c. Contieni gli esiti di Amazon Inspector relativi alla funzione Lambda coinvolta nell'esito.

Gestione di più account in Amazon GuardDuty

Se il tuo AWS ambiente ha più account, puoi gestirli designando un AWS account come account amministratore. È quindi possibile associare altri AWS account a questo account amministratore come account membro. Questo account GuardDuty amministratore designato può configurare i piani di protezione. GuardDuty Esistono due modi per associare gli account a un account amministratore: creare un'organizzazione utilizzando AWS Organizations e sia l'account amministratore che uno o più account membro appartengono a questa organizzazione, oppure inviare un invito a un AWS account tramite GuardDuty.

GuardDuty consiglia di utilizzare il AWS Organizations metodo. Per ulteriori informazioni sulla configurazione di un'organizzazione, consulta Creazione di un'organizzazione nella Guida per l'utente di AWS Organizations .

Gestione di più account con AWS Organizations

Se l'account che desideri specificare come account GuardDuty amministratore fa parte di un'organizzazione in AWS Organizations, puoi specificare quell'account come amministratore delegato dell'organizzazione per GuardDuty. L'account registrato come amministratore delegato diventa automaticamente l'account GuardDuty amministratore.

Puoi utilizzare questo account amministratore GuardDuty per abilitare e gestire qualsiasi utente Account AWS dell'organizzazione quando aggiungi quell'account come account membro.

Se disponi già di un account GuardDuty amministratore con account membro associati su invito, puoi registrare quell'account come amministratore GuardDuty delegato dell'organizzazione. Quando lo fai, tutti gli account membro attualmente associati rimangono membri, consentendoti di sfruttare appieno le funzionalità aggiuntive di gestione dei tuoi GuardDuty account con AWS Organizations.

Per ulteriori informazioni sul supporto di più account GuardDuty tramite un'organizzazione, consultaGestione GuardDuty degli account con AWS Organizations.

Gestione di più account tramite invito

Se gli account che desideri associare non fanno parte della tua organizzazione, puoi specificare un account amministratore in GuardDuty e quindi utilizzare l'account amministratore per invitare altri

utenti Account AWS a diventare membri degli account. Quando l'account invitato accetta l'invito, tale account diventa un account GuardDuty membro associato all'account amministratore.

Per ulteriori informazioni sul supporto di più account su invito, GuardDuty consultaGestione GuardDuty degli account su invito.

Comprensione della relazione tra account GuardDuty amministratore e account membro

Quando si utilizza GuardDuty in un ambiente con più account, l'account amministratore può gestire determinati aspetti per GuardDuty conto degli account dei membri. Le funzioni principali che l'account amministratore può eseguire sono:

- Aggiungere e rimuovere gli account membri associati. Il processo di esecuzione varia in base al fatto che gli account siano associati tramite organizzazioni o tramite invito.
- Gestisci lo stato degli account dei GuardDuty membri associati, incluse l'attivazione e la sospensione. GuardDuty

> **Note**
>
> Account amministrativi delegati gestiti con attivazione AWS Organizations GuardDuty automatica degli account aggiunti come membri.

- Personalizza i risultati all'interno della GuardDuty rete attraverso la creazione e la gestione di regole di soppressione, elenchi di IP affidabili ed elenchi di minacce. Gli account membri perdono l'accesso a queste funzionalità in un ambiente con più account.

La tabella seguente descrive in dettaglio la relazione tra account GuardDuty amministratore e account membro.

In questa tabella:

- Autonomo: un account può eseguire l'azione elencata solo per il proprio account.
- Qualsiasi: un account può eseguire l'azione elencata per qualsiasi account associato.
- Tutti: un account può eseguire l'azione elencata e questa si applica a tutti gli account associati. Di solito, l'account che esegue questa azione è un account GuardDuty amministratore designato

Le celle della tabella con un trattino (—) indicano che l'account non può eseguire l'azione elencata.

Action	Tramite AWS Organizations		Su invito	
	Account GuardDuty amministratore delegato	Account membro associato	Account GuardDuty amministratore delegato	Account membro associato
Enable GuardDuty	Any	–	Self	Self
Enable GuardDuty automatically for the entire organization (`ALL`, `NEW`, `NONE`)	All	–	–	–
View all Organizations member accounts regardless of GuardDuty status	Any	–	–	–
Generate sample findings	Self	Self	Self	Self
View all GuardDuty findings	Any	Self	Any	Self
Archive GuardDuty findings	Any	–	Any	–

Apply suppressi on rules	All	–	All	–
Create trusted IP list or threat lists	All	–	All	–
Update trusted IP list or threat lists	All	–	All	–
Delete trusted IP list or threat lists	All	–	All	–
Set EventBrid ge notification frequency	All	–	All	Self
Set Amazon S3 location for exporting findings	All	–	All	Self
Enable one or more optional protection plans for the entire organization (`ALL`, `NEW`, `NONE`)	All	–	–	–
Enable any GuardDuty protection plan for individual accounts	Any	–	Any	Self
Disassociate a member account	Any	–	Any	–

Disassociate from an administrator account account	–	Self[#]	–	Self
Delete a disassociated member account	Any	–	Any	–
Suspend GuardDuty	Any[*]	–	Any[*]	–
Disable GuardDuty	Any[*]	–	Any[*]	–

- # Indica che l'account può eseguire questa azione solo se l'account GuardDuty amministratore delegato non ha impostato la preferenza di attivazione automatica per `ALL` i membri dell'organizzazione.
- * Indica che questa azione deve essere eseguita per tutti gli account associati prima di essere eseguita per questo account. Dopo aver dissociato questi account, è necessario eliminarli. Per ulteriori informazioni sull'esecuzione di queste attività nella propria organizzazione, vedereMantenere la propria organizzazione all'interno GuardDuty.

Gestione GuardDuty degli account con AWS Organizations

Quando si utilizza GuardDuty con un' AWS organizzazione, l'account di gestione di tale organizzazione può designare qualsiasi account all'interno dell'organizzazione come account amministratore delegato GuardDuty . Per questo account amministratore, GuardDuty viene abilitato automaticamente solo nell'account designato. Regione AWS Questo account è inoltre autorizzato ad abilitare e gestire tutti GuardDuty gli account dell'organizzazione all'interno di quella regione. L'account amministratore può visualizzare e aggiungere membri a questa AWS organizzazione.

Se hai già impostato un account GuardDuty amministratore con account membro associati su invito e gli account membro fanno parte della stessa organizzazione, il loro tipo cambia da By Invitation a Via Organizations quando imposti un account GuardDuty amministratore delegato per la tua organizzazione. Se un account GuardDuty amministratore delegato ha precedentemente aggiunto

membri su invito che non fanno parte della stessa organizzazione, il relativo tipo rimane Per invito. In entrambi i casi, gli account aggiunti in precedenza sono account membro associati all'account GuardDuty amministratore delegato dell'organizzazione.

È possibile continuare ad aggiungere account come membri anche se non sono all'esterno dell'organizzazione. Per ulteriori informazioni, consulta Aggiunta e gestione degli account tramite invito o Designazione di un account GuardDuty amministratore delegato e gestione dei membri tramite la console GuardDuty .

Indice

- Considerazioni e consigli per la designazione di un account amministratore delegato GuardDuty
- Autorizzazioni necessarie per designare un account amministratore delegato GuardDuty
- Designazione di un account GuardDuty amministratore delegato e gestione dei membri tramite la console GuardDuty
- Designazione di un account GuardDuty amministratore GuardDuty delegato e gestione dei membri utilizzando l'API
- Mantenere la propria organizzazione all'interno GuardDuty
- Modifica dell'account amministratore delegato GuardDuty

Considerazioni e consigli per la designazione di un account amministratore delegato GuardDuty

Le considerazioni e i consigli seguenti possono aiutarti a capire come funziona un account GuardDuty amministratore delegato in: GuardDuty

Un account GuardDuty amministratore delegato può gestire un massimo di 50.000 membri.

> È previsto un limite di 50.000 account membro per account amministratore delegato GuardDuty . Ciò include gli account membro aggiunti tramite AWS Organizations o quelli che hanno accettato l'invito dell'account GuardDuty amministratore a entrare a far parte della propria organizzazione. Tuttavia, nella tua AWS organizzazione potrebbero esserci più di 50.000 account.
>
> Se superi il limite di 50.000 account membri, riceverai una notifica e un'e-mail all'account amministratore delegato designato GuardDuty . CloudWatch AWS Health Dashboard

Un account GuardDuty amministratore delegato è regionale.

Al contrario AWS Organizations, GuardDuty è un servizio regionale. Gli account di GuardDuty amministratore delegato e i relativi account membro devono essere aggiunti AWS Organizations in ogni regione desiderata in cui è stata GuardDuty abilitata. Se l'account di gestione dell'organizzazione designa un account GuardDuty amministratore delegato solo negli Stati Uniti orientali (Virginia settentrionale), l'account GuardDuty amministratore delegato gestirà solo gli account dei membri aggiunti all'organizzazione in quella regione. Per ulteriori informazioni sulla parità di funzionalità nelle regioni in cui GuardDuty è disponibile, consulta. Regioni ed endpoint

Casi speciali per le regioni che hanno aderito all'iniziativa

- Quando un account GuardDuty amministratore delegato disattiva un'area di attivazione, anche se l'organizzazione ha la configurazione di GuardDuty attivazione automatica impostata su Solo nuovi account membro (`NEW`) o su tutti gli account membro (`ALL`), GuardDuty non può essere abilitata per nessun account membro dell'organizzazione attualmente disabilitato. GuardDuty Per informazioni sulla configurazione degli account membro, apri Account nel riquadro di navigazione della GuardDuty console o utilizza l'API. ListMembers
- Quando lavori con la configurazione di GuardDuty attivazione automatica impostata su`NEW`, assicurati che sia soddisfatta la seguente sequenza:

  1. Gli account dei membri aderiscono a una regione opt-in.
  2. Aggiungi gli account dei membri alla tua organizzazione in. AWS Organizations

  Se modifichi l'ordine di questi passaggi, l'impostazione di GuardDuty attivazione automatica con non **`NEW`** funzionerà nella regione di attivazione specifica perché l'account membro non è più nuovo per l'organizzazione. GuardDuty offre due soluzioni alternative:

  - Imposta la configurazione di GuardDuty attivazione automatica su`ALL`, che include account membri nuovi ed esistenti. In questo caso, l'ordine di questi passaggi non è rilevante.
  - Se un account membro fa già parte della tua organizzazione, gestisci la GuardDuty configurazione di questo account individualmente nella regione di attivazione specifica utilizzando la GuardDuty console o l'API.

Si consiglia a un' AWS organizzazione di avere lo stesso account GuardDuty amministratore delegato in tutti i. Regioni AWS

Ti consigliamo di designare lo stesso account GuardDuty amministratore delegato per la tua organizzazione in tutti i paesi in Regioni AWS cui hai abilitato. GuardDuty Se si designa un account come account GuardDuty amministratore delegato in una regione, si consiglia di utilizzare lo stesso account dell'account GuardDuty amministratore delegato in tutte le altre regioni.

È possibile designare un nuovo account GuardDuty amministratore delegato in qualsiasi momento. Per ulteriori informazioni sulla rimozione dell'account GuardDuty amministratore delegato esistente, consulta. Modifica dell'account amministratore delegato GuardDuty

Non è consigliabile impostare l'account di gestione dell'organizzazione come account GuardDuty amministratore delegato.

L'account di gestione dell'organizzazione può essere l'account GuardDuty amministratore delegato. Tuttavia, le best practice di sicurezza AWS seguono il principio del privilegio minimo e sconsigliano questa configurazione.

La modifica di un account GuardDuty amministratore delegato non disabilita gli account GuardDuty dei membri.

Se rimuovi un account GuardDuty amministratore delegato, GuardDuty rimuove tutti gli account membro associati a tale account amministratore delegato GuardDuty . GuardDuty rimane comunque abilitato per tutti questi account membro.

Autorizzazioni necessarie per designare un account amministratore delegato GuardDuty

Quando si delega un account GuardDuty amministratore delegato, è necessario disporre delle autorizzazioni per l'attivazione GuardDuty e di determinate azioni API. AWS Organizations Puoi aggiungere la seguente istruzione alla fine di una policy IAM esistente per concedere queste autorizzazioni:

```
{
    "Sid": "PermissionsForGuardDutyAdmin",
    "Effect": "Allow",
    "Action": [
        "guardduty:EnableOrganizationAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
```

```
    "Resource": "*"
}
```

Inoltre, se desideri designare il tuo account di AWS Organizations gestione come account GuardDuty amministratore GuardDuty delegato, tale entità avrà bisogno delle autorizzazioni per l'inizializzazione. `CreateServiceLinkedRole` GuardDuty A tale scopo, aggiungi la seguente dichiarazione alla policy IAM e sostituisci *111122223333* con l' Account AWS ID dell'account di gestione della tua organizzazione:

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

Designazione di un account GuardDuty amministratore delegato e gestione dei membri tramite la console GuardDuty

Indice

- Fase 1: designare un GuardDuty account amministratore delegato per l'organizzazione
- Fase 2 — Configurazione delle preferenze di attivazione automatica per l'organizzazione
- Fase 3: aggiungere account all'organizzazione come membri
- (Facoltativo) passo 4: configura i piani di protezione per i singoli account

Fase 1: designare un GuardDuty account amministratore delegato per l'organizzazione

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

Per accedere, utilizza le credenziali dell'account di gestione della tua organizzazione AWS Organizations .

2. Se hai già abilitato GuardDuty l'account di gestione, salta questo passaggio e segui il passaggio successivo.

   Se non l'hai GuardDuty ancora abilitato, seleziona Inizia, quindi designa un account GuardDuty amministratore delegato nella pagina Benvenuto. GuardDuty

   > **Note**
   >
   > L'account di gestione deve avere il ruolo GuardDuty collegato al servizio (SLR) in modo che l'account GuardDuty amministratore delegato possa attivarlo e gestirlo. GuardDuty Una volta abilitato GuardDuty in una regione l'account di gestione, questa SLR viene creata automaticamente.

3. Esegui questo passaggio dopo aver abilitato GuardDuty l'account di gestione. Nel pannello di navigazione della GuardDuty console, scegli Impostazioni. Nella pagina Impostazioni, inserisci l' Account AWS ID a 12 cifre dell'account che desideri designare come account GuardDuty amministratore delegato per l'organizzazione.

   Assicurati di abilitarlo GuardDuty per il tuo account GuardDuty amministratore delegato appena designato, altrimenti non sarà in grado di intraprendere alcuna azione.

4. Scegli Delega.

5. (Consigliato) Ripeti il passaggio precedente per designare l'account GuardDuty amministratore delegato in ogni account in Regione AWS cui hai abilitato. GuardDuty

Fase 2 — Configurazione delle preferenze di attivazione automatica per l'organizzazione

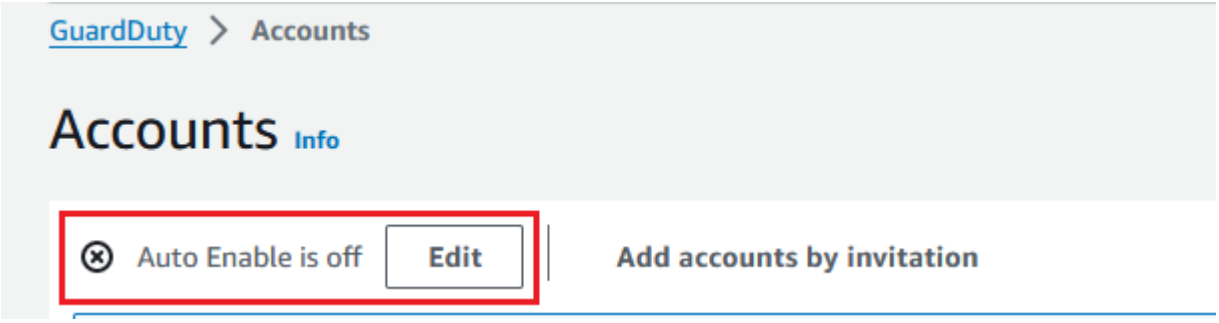
1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Per accedere, utilizza le credenziali GuardDuty dell'account amministratore.

2. Dal riquadro di navigazione, selezionare Accounts (Account).

La pagina Account fornisce opzioni di configurazione per l'account GuardDuty amministratore da abilitare automaticamente GuardDuty e i piani di protezione opzionali per conto degli account membri che appartengono all'organizzazione.

3. Per aggiornare le impostazioni di attivazione automatica esistenti, scegli Modifica.



Questo supporto è disponibile per la configurazione GuardDuty e per tutti i piani di protezione opzionali supportati nel tuo. Regione AWS Puoi selezionare una delle seguenti opzioni di configurazione per GuardDuty conto dei tuoi account membro:

- Abilita per tutti gli account (**`ALL`**): seleziona questa opzione per abilitare l'opzione corrispondente per tutti gli account di un'organizzazione. inclusi i nuovi account che entrano a far parte dell'organizzazione e gli account che potrebbero essere stati sospesi o rimossi dall'organizzazione. Ciò include anche l'account GuardDuty amministratore delegato.

  > **Note**
  >
  > Potrebbero essere necessarie fino a 24 ore per aggiornare la configurazione di tutti gli account membri.

- Attivazione automatica per nuovi account (**`NEW`**): seleziona questa opzione per abilitare GuardDuty automaticamente i piani di protezione opzionali solo per i nuovi account membri quando entrano a far parte dell'organizzazione.
- Non abilitare (**`NONE`**): seleziona questa opzione per impedire l'attivazione dell'opzione corrispondente per i nuovi account dell'organizzazione. In questo caso, l'account GuardDuty amministratore gestirà ogni account singolarmente.

  Quando aggiorni l'impostazione di attivazione automatica da `ALL` o `NEW` versoNONE, questa azione non disattiva l'opzione corrispondente per i tuoi account esistenti. Questa configurazione verrà applicata ai nuovi account che entrano a far parte dell'organizzazione.

Dopo aver aggiornato le impostazioni di attivazione automatica, nessun nuovo account avrà l'opzione corrispondente abilitata.

> **Note**
>
> Quando un account GuardDuty amministratore delegato disattiva un'area di attivazione, anche se l'organizzazione ha la configurazione di GuardDuty attivazione automatica impostata su Solo nuovi account membro (`NEW`) o su tutti gli account membro (`ALL`), GuardDuty non può essere abilitata per nessun account membro dell'organizzazione attualmente disabilitato. GuardDuty Per informazioni sulla configurazione degli account membro, apri Account nel riquadro di navigazione della GuardDuty console o utilizza l'API. ListMembers

4. Seleziona Salvataggio delle modifiche.
5. (Facoltativo) se desideri utilizzare le stesse preferenze in ogni regione, aggiorna le preferenze in ciascuna delle regioni supportate separatamente.

   Alcuni dei piani di protezione opzionali potrebbero non essere disponibili in tutti i paesi in Regioni AWS cui GuardDuty sono disponibili. Per ulteriori informazioni, consulta Regioni ed endpoint.

Fase 3: aggiungere account all'organizzazione come membri

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Per accedere, utilizza le credenziali GuardDuty dell'account amministratore delegato.
2. Dal riquadro di navigazione, selezionare Accounts (Account).

   La tabella degli account mostra tutti gli account aggiunti Tramite l'organizzazione (AWS Organizations) o Tramite invito. Se un account membro non è associato all'account GuardDuty amministratore dell'organizzazione, lo stato di tale account membro è Non membro.
3. Seleziona uno o più ID account che desideri aggiungere come membri. Questi ID account devono avere il Tipo impostato su Tramite l'organizzazione.

   Gli account aggiunti tramite invito non fanno parte dell'organizzazione. Puoi gestire tali account singolarmente. Per ulteriori informazioni, consulta Gestione degli account tramite invito.
4. Scegli il menu a discesa Operazioni, quindi Aggiungi membro. Dopo aver aggiunto questo account come membro, verrà applicata la GuardDuty configurazione di attivazione automatica.

In base alle impostazioni dithe section called “Fase 1: designare un GuardDuty account amministratore delegato per l'organizzazione”, la GuardDuty configurazione di questi account potrebbe cambiare.

5. Puoi selezionare la freccia rivolta verso il basso della colonna Stato per ordinare gli account in base allo stato Non sono un membro e quindi scegliere ogni account che non è GuardDuty abilitato nella regione corrente.

   Se nessuno degli account elencati nella tabella degli account è stato ancora aggiunto come membro, puoi abilitarlo GuardDuty nella regione corrente per tutti gli account dell'organizzazione. Scegli Abilita nel banner nella parte superiore della pagina. Questa azione attiva automaticamente la GuardDuty configurazione di attivazione automatica in modo che GuardDuty venga abilitata per ogni nuovo account che si unisce all'organizzazione.

6. Scegli Conferma per aggiungere gli account come membri. Questa azione si attiva anche GuardDuty per tutti gli account selezionati. Lo Stato degli account cambia in Abilitato.

7. (Consigliato) Ripeti questi passaggi in ciascuno di essi Regione AWS. Ciò garantisce che l'account GuardDuty amministratore delegato possa gestire i risultati e altre configurazioni per gli account dei membri in tutte le regioni in cui è stata GuardDuty abilitata.

   La funzionalità di attivazione automatica abilita tutti GuardDuty i futuri membri della tua organizzazione. Ciò consente GuardDuty all'account amministratore delegato di gestire tutti i nuovi membri creati all'interno dell'organizzazione o aggiunti all'organizzazione. Quando il numero di account membri raggiunge il limite di 50.000, la funzione di attivazione automatica viene disattivata automaticamente. Se rimuovi un account membro e il numero totale di membri scende a meno di 50.000, la funzione di attivazione automatica si riattiva.

(Facoltativo) passo 4: configura i piani di protezione per i singoli account

Puoi configurare piani di protezione per singoli account tramite la pagina Account.

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Utilizza le credenziali GuardDuty dell'account amministratore delegato.

2. Dal riquadro di navigazione, selezionare Accounts (Account).

3. Seleziona uno o più account per i quali desideri configurare un piano di protezione. Ripeti i seguenti passaggi per ogni piano di protezione da configurare:

   a. Scegli Modifica piani di protezione.

b. Dall'elenco dei piani di protezione, scegli quello da configurare.

c. Scegli una delle operazioni che desideri eseguire per questo piano di protezione, quindi scegli Conferma.

d. Per l'account selezionato, la colonna corrispondente al piano di protezione configurato mostrerà la configurazione aggiornata come Abilitata o Non abilitata.

Designazione di un account GuardDuty amministratore GuardDuty delegato e gestione dei membri utilizzando l'API

Indice

- Fase 1: designare un GuardDuty account amministratore delegato per l'organizzazione AWS
- Fase 2: configurazione delle preferenze di abilitazione automatica per l'organizzazione
- Fase 3: aggiungere account all'organizzazione come membri

Fase 1: designare un GuardDuty account amministratore delegato per l'organizzazione AWS

1. Esegui enableOrganizationAdminAccountutilizzando le credenziali dell'account Account AWS di gestione dell'organizzazione.

   - In alternativa, puoi usare AWS Command Line Interface per farlo. Il AWS CLI comando seguente designa un account GuardDuty amministratore delegato solo per la regione corrente. Esegui il AWS CLI comando seguente e assicurati di sostituire *1111* con l' Account AWS ID dell'account che desideri designare come account amministratore delegato: GuardDuty

     ```
     aws guardduty enable-organization-admin-account --admin-account-id 111111111111
     ```

     Per designare l'account GuardDuty amministratore delegato per altre regioni, specifica la regione nel comando. AWS CLI L'esempio seguente mostra come abilitare un account GuardDuty amministratore delegato negli Stati Uniti occidentali (Oregon). Assicurati di sostituire *us-west-2* con la regione per la quale desideri assegnare l'account amministratore delegato. GuardDuty GuardDuty

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111
 --region us-west-2
```

Per informazioni su Regioni AWS dove GuardDuty è disponibile, consulta. Regioni ed endpoint

Se non GuardDuty è abilitato per il tuo account GuardDuty amministratore delegato, non sarà in grado di eseguire alcuna azione. Se non l'hai già fatto, assicurati di abilitarlo GuardDuty per il nuovo GuardDuty account amministratore delegato designato.

2. (Consigliato) Ripeti il passaggio precedente per designare l'account GuardDuty amministratore delegato in ogni account in Regione AWS cui hai abilitato. GuardDuty

Fase 2: configurazione delle preferenze di abilitazione automatica per l'organizzazione

1. 1. Esegui UpdateOrganizationConfigurationutilizzando le credenziali dell'account GuardDuty amministratore delegato, per configurare automaticamente GuardDuty e i piani di protezione opzionali in quella regione per la tua organizzazione

   Per trovare i dati `detectorId` relativi al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

   > **Note**
   >
   > Per informazioni sulle varie configurazioni di attivazione automatica, vedere autoEnableOrganization Membri.

   2. Per impostare le preferenze di abilitazione automatica per uno qualsiasi dei piani di protezione facoltativi supportati nella tua regione, segui i passaggi riportati nelle sezioni della documentazione corrispondenti a ciascun piano di protezione.
   3. Puoi convalidare le preferenze per la tua organizzazione nella regione attuale. Esegui describeOrganizationConfiguration. Assicurati di specificare l'ID del rilevatore dell'account amministratore delegato GuardDuty .

> **Note**
>
> L'aggiornamento della configurazione per tutti gli account membri può richiedere fino a 24 ore.

- 1. In alternativa, esegui il AWS CLI comando seguente per impostare le preferenze da abilitare o disabilitare automaticamente GuardDuty in quella regione per i nuovi account (`NEW`) che entrano a far parte dell'organizzazione, per tutti gli account (`ALL`) o per nessuno degli account (`NONE`) dell'organizzazione. Per ulteriori informazioni, consulta autoEnableOrganizationMembri. In base alle tue preferenze, potrebbe essere necessario sostituire `NEW` con `ALL` o `NONE`. Se si configura il piano di protezione con`ALL`, il piano di protezione verrà abilitato anche per l'account GuardDuty amministratore delegato. Assicurati di specificare l'ID del rilevatore dell'account GuardDuty amministratore delegato che gestisce la configurazione dell'organizzazione.

  Per trovare il codice `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
  ```

  2. Puoi convalidare le preferenze per la tua organizzazione nella regione attuale. Esegui il AWS CLI comando seguente utilizzando l'ID del rilevatore dell' GuardDuty account amministratore delegato.

  ```
  aws guardduty describe-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0
  ```

2. (Consigliato) ripeti i passaggi precedenti in ogni regione utilizzando l'ID del rilevatore dell'account GuardDuty amministratore delegato.

> **Note**
>
> Quando un account GuardDuty amministratore delegato disattiva un'area di attivazione, anche se l'organizzazione ha la configurazione di GuardDuty attivazione automatica impostata su Solo nuovi account membro (`NEW`) o su tutti gli account membro (`ALL`), GuardDuty non può essere abilitata per nessun account membro dell'organizzazione

attualmente disabilitato. GuardDuty Per informazioni sulla configurazione degli account membro, apri Account nel riquadro di navigazione della GuardDuty console o utilizza l'API. ListMembers

Fase 3: aggiungere account all'organizzazione come membri

- Esegui CreateMembersutilizzando le credenziali dell'account GuardDuty amministratore delegato indicato nel passaggio precedente.

  È necessario specificare l'ID del rilevatore regionale dell'account GuardDuty amministratore delegato e i dettagli dell'account (Account AWS ID e indirizzi e-mail corrispondenti) degli account che si desidera aggiungere come membri. GuardDuty È possibile creare uno o più membri con questa operazione API.

  Quando lavori CreateMembers nella tua organizzazione, le preferenze di attivazione automatica per i nuovi membri verranno applicate quando nuovi account membro entrano a far parte dell'organizzazione. Se utilizzi CreateMembers un account membro esistente, la configurazione dell'organizzazione verrà applicata anche ai membri esistenti. Ciò potrebbe modificare la configurazione attuale degli account dei membri esistenti.

  Eseguilo ListAccountsnell'AWS Organizations API Reference, per visualizzare tutti gli account dell' AWS organizzazione.

  > **Important**
  >
  > Quando aggiungi un account come GuardDuty membro, questo verrà automaticamente GuardDuty abilitato in quella regione. Esiste un'eccezione relativamente all'account di gestione dell'organizzazione. Prima che l'account dell'account di gestione venga aggiunto come GuardDuty membro, deve essere GuardDuty abilitato.

- In alternativa, puoi usare AWS Command Line Interface. Esegui il comando AWS CLI seguente e assicurati di utilizzare il tuo ID rilevatore, l'ID Account AWS e l'indirizzo e-mail validi associati all'ID account.

  Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-details AccountId=111122223333,Email=guardduty-member-name@amazon.com
```

È possibile visualizzare un elenco di tutti i membri dell'organizzazione eseguendo il AWS CLI comando seguente:

```
aws organizations list-accounts
```

Dopo aver aggiunto questo account come membro, verrà applicata la GuardDuty configurazione di attivazione automatica.

Mantenere la propria organizzazione all'interno GuardDuty

In qualità di account GuardDuty amministratore delegato, sei responsabile del mantenimento della configurazione GuardDuty e dei relativi piani di protezione opzionali per tutti gli account dell'organizzazione supportati. Regione AWS Le seguenti sezioni forniscono le opzioni relative al mantenimento dello stato di configurazione GuardDuty o di uno qualsiasi dei relativi piani di protezione opzionali:

Per mantenere lo stato di configurazione dell'intera organizzazione in ogni regione

- Imposta le preferenze di attivazione automatica per l'intera organizzazione utilizzando la GuardDuty console: puoi abilitarla GuardDuty automaticamente per tutti (`ALL`) i membri dell'organizzazione o per i nuovi (`NEW`) membri che si uniscono all'organizzazione, oppure scegliere di non (`NONE`) abilitare automaticamente nessuno dei membri dell'organizzazione.

  Puoi anche configurare le stesse impostazioni o impostazioni diverse per tutti i piani di protezione inclusi. GuardDuty

  Potrebbero essere necessarie fino a 24 ore per aggiornare la configurazione di tutti gli account membri dell'organizzazione.
- Aggiorna le preferenze di attivazione automatica utilizzando l'API — Run UpdateOrganizationConfigurationto configura automaticamente GuardDuty e i relativi piani di protezione opzionali per l'organizzazione. Quando corri CreateMembersad aggiungere nuovi account membro nella tua organizzazione, le impostazioni configurate verranno applicate automaticamente. Se utilizzi CreateMembers un account membro esistente, la configurazione

dell'organizzazione verrà applicata anche ai membri esistenti. Ciò potrebbe modificare la configurazione attuale degli account dei membri esistenti.

Per visualizzare tutti gli account della tua organizzazione, ListAccountsesegui l'AWS Organizations API Reference.

Per mantenere lo stato di configurazione per i singoli account dei membri in ciascuna regione

- Per visualizzare tutti gli account della tua organizzazione, ListAccountsesegui l'AWS Organizations API Reference.
- Se desideri che gli account membro selettivi abbiano uno stato di configurazione diverso, esegui l'operazione UpdateMemberDetectorsper ogni account membro singolarmente.

  Puoi utilizzare la GuardDuty console per eseguire la stessa operazione accedendo alla pagina Account della console. GuardDuty

  Per informazioni sull'attivazione dei piani di protezione per singoli account utilizzando la console o l'API, consulta la pagina di configurazione per il piano di protezione corrispondente.

Modifica dell'account amministratore delegato GuardDuty

Puoi modificare l'account GuardDuty amministratore delegato per la tua organizzazione in ogni regione e quindi delegare un nuovo amministratore in ogni regione. Per mantenere un livello di sicurezza per gli account dei membri dell'organizzazione in una regione, è necessario disporre di un account GuardDuty amministratore delegato in quella regione.

Rimozione dell'account amministratore delegato GuardDuty esistente

Fase 1 - Rimuovere l'account GuardDuty amministratore delegato esistente in ogni regione

1. Come account GuardDuty amministratore delegato esistente, elenca tutti gli account membro associati al tuo account amministratore. Corri ListMembersconOnlyAssociated=false.
2. Se la preferenza di attivazione automatica per GuardDuty o per uno qualsiasi dei piani di protezione opzionali è impostata suALL, esegui UpdateOrganizationConfigurationper aggiornare la configurazione dell'organizzazione su uno dei due NEW piani di protezione opzionali. NONE Questa azione eviterà che si verifichi un errore quando si dissociano tutti gli account dei membri nel passaggio successivo.

3. Esegui DisassociateMembersper dissociare tutti gli account membro associati all'account amministratore.
4. Esegui DeleteMembersper eliminare le associazioni tra l'account amministratore e gli account dei membri.
5. Come account di gestione dell'organizzazione, esegui DisableOrganizationAdminAccountper rimuovere l'account GuardDuty amministratore delegato esistente.
6. Ripeti questi passaggi in ognuno dei Regione AWS paesi in cui hai questo GuardDuty account amministratore delegato.

Fase 2 - Annullare la registrazione GuardDuty dell'account amministratore delegato esistente in AWS Organizations (azione globale una tantum)

- Esegui DeregisterDelegatedAdministratornell'AWS Organizations API Reference, per annullare la registrazione dell'account amministratore delegato GuardDuty esistente in. AWS Organizations

  In alternativa, puoi eseguire il seguente AWS CLI comando:

  ```
  aws organizations deregister-delegated-administrator --account-id 111122223333 --
  service-principal guardduty.amazonaws.com
  ```

  Assicurati di sostituire *111122223333* con l'account amministratore delegato GuardDuty esistente.

  Dopo aver annullato la registrazione del vecchio account GuardDuty amministratore delegato, puoi aggiungerlo come account membro al nuovo account amministratore delegato. GuardDuty

Designazione di un nuovo account amministratore delegato GuardDuty in ogni regione

1. Designare un nuovo account GuardDuty amministratore delegato in ciascuna regione utilizzando uno dei seguenti metodi di accesso:
   - Utilizzo della GuardDuty console:. Fase 1: designare un GuardDuty account amministratore delegato per l'organizzazione
   - Utilizzo GuardDuty dell'API —Fase 1: designare un GuardDuty account amministratore delegato per l'organizzazione AWS.

2. Esegui DescribeOrganizationConfigurationper visualizzare l'attuale configurazione di attivazione automatica per la tua organizzazione.

> **Important**
>
> Prima di aggiungere membri al nuovo account GuardDuty amministratore delegato, è necessario verificare la configurazione di attivazione automatica per l'organizzazione. Questa configurazione è specifica del nuovo account GuardDuty amministratore delegato e della regione selezionata e non si riferisce a. AWS Organizations Quando si aggiunge un account membro dell'organizzazione (nuovo o esistente) al nuovo account GuardDuty amministratore delegato, la configurazione di attivazione automatica del nuovo account GuardDuty amministratore delegato verrà applicata al momento dell'attivazione GuardDuty o di uno qualsiasi dei suoi piani di protezione opzionali.

Per modificare questa configurazione dell'organizzazione per il nuovo account GuardDuty amministratore delegato, utilizza uno dei seguenti metodi di accesso:

- Utilizzo GuardDuty della console:Fase 2 — Configurazione delle preferenze di attivazione automatica per l'organizzazione.
- Utilizzo GuardDuty dell'API —Fase 2: configurazione delle preferenze di abilitazione automatica per l'organizzazione.

Gestione GuardDuty degli account su invito

Per gestire gli account esterni all'organizzazione, è possibile utilizzare il metodo di invito legacy. Quando utilizzi questo metodo, il tuo account viene designato come account amministratore nel momento in cui un altro account accetta l'invito a diventare un account membro.

Se il tuo account non è un account amministratore, puoi accettare un invito da un altro account. Quando accetti l'invito, il tuo account diventa un account membro. Un AWS account non può essere contemporaneamente un account GuardDuty amministratore e un account membro.

Quando accetti un invito da un account, non puoi accettare un invito da un altro account. Per accettare un invito da un altro account, devi prima dissociare il tuo account dall'account amministratore esistente. In alternativa, l'account amministratore può anche dissociare e rimuovere il tuo account dalla sua organizzazione.

Gli account associati su invito hanno lo stesso account-to-member rapporto di amministratore complessivo degli account associati da AWS Organizations, come descritto in[Comprensione della relazione tra account GuardDuty amministratore e account membro](). Tuttavia, gli utenti con account amministratore a inviti non possono abilitare GuardDuty gli account dei membri associati o visualizzare altri account non membri all'interno della propria AWS Organizations organizzazione.

> **Important**
>
> Quando si GuardDuty creano account membri utilizzando questo metodo, può verificarsi un trasferimento di dati interregionale. Per verificare gli indirizzi e-mail degli account dei membri, GuardDuty utilizza un servizio di verifica e-mail che opera solo nella regione degli Stati Uniti orientali (Virginia settentrionale).

Aggiunta e gestione degli account tramite invito

Scegli uno dei metodi di accesso per aggiungere e invitare account a diventare account GuardDuty membro come account GuardDuty amministratore.

Console

Fase 1: aggiunta di un account

1. Apri la GuardDuty console all'[indirizzo https://console.aws.amazon.com/guardduty/]().
2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Scegli Aggiungi account tramite invito nel riquadro superiore.
4. Nella pagina Aggiungi account membro, in Inserisci i dettagli dell'account, inserisci l' Account AWS ID e l'indirizzo email associati all'account che desideri aggiungere.
5. Per aggiungere un'altra riga in cui immettere i dettagli dell'account uno alla volta, scegli Aggiungi un altro account. Puoi anche scegliere Carica il file .csv con i dettagli dell'account per aggiungere account in blocco.

   > **Important**
   >
   > La prima riga del file csv deve contenere l'intestazione, come illustrato nell'esempio seguente: `Account ID,Email`. Ogni riga successiva deve contenere un unico Account AWS ID valido e l'indirizzo e-mail associato. Il formato di una riga è valido

se contiene un solo Account AWS ID e l'indirizzo e-mail associato separati da una virgola.

```
Account ID,Email
                                555555555555,user@example.com
```

6. Dopo aver aggiunto tutti i dettagli degli account, scegli Successivo. Puoi visualizzare gli account appena aggiunti nella tabella Account. Lo Stato di questi account sarà Invito non inviato. Per informazioni sull'invio di un invito a uno o più account aggiunti, consulta Step 2 - Invite an account.

Fase 2: invito di un account

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Seleziona uno o più account che desideri invitare su Amazon GuardDuty.
4. Scegli il menu a discesa Operazioni, quindi Invita.
5. Nella GuardDuty finestra di dialogo Invito a, inserisci un messaggio di invito (opzionale).

   Se l'account invitato non ha accesso all'e-mail, seleziona la casella di controllo Invia anche una notifica e-mail all'utente root nell' Account AWS dell'invitato e genera un avviso nel AWS Health Dashboard.
6. Selezionare Send invitation (Invia invito). Se gli invitati hanno accesso all'indirizzo e-mail specificato, possono visualizzare l'invito aprendo la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
7. Quando un invitato accetta l'invito, il valore nella colonna Stato cambia in Invitato. Per informazioni sull'accettazione di un invito, consulta Step 3 - Accept an invitation.

Fase 3: accettazione di un invito

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

> **Important**
>
> È necessario abilitarla GuardDuty prima di poter visualizzare o accettare un invito all'iscrizione.

2. Effettua le seguenti operazioni solo se non l'hai GuardDuty ancora abilitato; in caso contrario, puoi saltare questo passaggio e continuare con il passaggio successivo.

   Se non l'hai ancora abilitato GuardDuty, scegli Get Started sulla GuardDuty pagina Amazon.

   Nella GuardDuty pagina Benvenuto, scegli Abilita GuardDuty.

3. Dopo aver abilitato GuardDuty il tuo account, segui la procedura seguente per accettare l'invito all'iscrizione:

   a. Nel pannello di navigazione scegli Impostazioni.

   b. Scegli Account.

   c. In Account, assicurati di verificare il proprietario dell'account dal quale accetti l'invito. Attiva Accetta per accettare l'invito.

4. Dopo aver accettato l'invito, il tuo account diventa un account GuardDuty membro. L'account il cui proprietario ha inviato l'invito diventa l'account GuardDuty amministratore. L'account amministratore saprà che hai accettato l'invito. La tabella Account GuardDuty del relativo account verrà aggiornata. Il valore nella colonna Stato corrispondente all'ID del tuo account membro cambierà in Abilitato. Il proprietario dell'account amministratore può ora visualizzare GuardDuty e gestire le configurazioni del piano di protezione per conto del tuo account. L'account amministratore può anche visualizzare e gestire i GuardDuty risultati generati per il tuo account membro.

API/CLI

Puoi designare un account GuardDuty amministratore e creare o aggiungere account GuardDuty membro su invito tramite le operazioni API. Esegui le seguenti operazioni GuardDuty API per designare l'account amministratore e gli account membro in. GuardDuty

Completa la procedura seguente utilizzando le credenziali dell' Account AWS account che desideri designare come amministratore. GuardDuty

Creazione o aggiunta di account membri

1. Esegui l'operazione CreateMembersAPI utilizzando le credenziali dell' AWS account abilitato. GuardDuty Questo è l'account che desideri utilizzare come GuardDuty account amministratore.

   È necessario specificare l'ID del rilevatore dell' AWS account corrente e l'ID account e l'indirizzo e-mail degli account di cui si desidera diventare GuardDuty membri. È possibile creare uno o più membri con questa operazione API.

   Puoi anche utilizzare gli strumenti della riga di AWS comando per designare un account amministratore eseguendo il seguente comando CLI. Assicurati di utilizzare il tuo ID rilevatore valido, l'ID account e l'e-mail.

   Per trovare l'indirizzo `detectorId` per il tuo account e la regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

   ```
   aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   account-details AccountId=111122223333,Email=guardduty-member@organization.com
   ```

2. Esegui InviteMembersutilizzando le credenziali dell' AWS account che hai GuardDuty abilitato. Questo è l'account che desideri utilizzare come GuardDuty account amministratore.

   È necessario specificare l'ID del rilevatore dell' AWS account corrente e gli ID degli account di cui si desidera diventare GuardDuty membri. È possibile invitare uno o più membri con questa operazione API.

   > **Note**
   >
   > È anche possibile specificare un messaggio di invito facoltativo tramite il parametro di richiesta `message`.

   È inoltre possibile AWS Command Line Interface utilizzarlo per designare gli account dei membri eseguendo il comando seguente. Assicurarsi di utilizzare l'ID rilevatore valido e gli ID account validi per gli account che desideri invitare.

   Per trovare i dati `detectorId` relativi al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 111122223333
```

Accettazione degli inviti

Completa la procedura seguente utilizzando le credenziali di ogni AWS account che desideri designare come account GuardDuty membro.

1. Esegui l'operazione CreateDetectorAPI per ogni AWS account che è stato invitato a diventare un account GuardDuty membro e per il quale desideri accettare un invito.

   È necessario specificare se la risorsa del rilevatore deve essere abilitata utilizzando il GuardDuty servizio. Un rilevatore deve essere creato e abilitato per GuardDuty diventare operativo. È necessario abilitarlo GuardDuty prima di accettare un invito.

   È inoltre possibile eseguire questa operazione utilizzando gli strumenti della riga di AWS comando utilizzando il seguente comando CLI.

   ```
   aws guardduty create-detector --enable
   ```

2. Esegui l'operazione AcceptAdministratorInvitationAPI per ogni AWS account per il quale desideri accettare l'invito all'iscrizione, utilizzando le credenziali di quell'account.

   Devi specificare l'ID del rilevatore di questo AWS account per l'account membro, l'ID account dell'account amministratore che ha inviato l'invito e l'ID dell'invito che stai accettando. È possibile trovare l'ID account dell'account amministratore dall'e-mail di invito o utilizzando l'operazione ListInvitations dell'API.

   Puoi anche accettare un invito utilizzando AWS Command Line Tools eseguendo il seguente comando CLI. Assicurati di utilizzare ID rilevatore, ID account amministratore e ID invito validi.

   Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

   ```
   aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --administrator-id 444455556666 --invitation-
   id 84b097800250d17d1872b34c4daadcf5
   ```

Consolidamento degli account di GuardDuty amministratore in un unico account di amministratore delegato GuardDuty dell'organizzazione

GuardDuty consiglia di utilizzare l'associazione attraverso AWS Organizations per gestire gli account dei membri con un account amministratore delegato. GuardDuty È possibile utilizzare il processo di esempio descritto di seguito per consolidare l'account amministratore e il membro associato su invito in un'organizzazione in un unico account amministratore GuardDuty delegato GuardDuty .

> **Note**
>
> Gli account che sono già gestiti da un account GuardDuty amministratore delegato o gli account dei membri attivi associati all'account GuardDuty amministratore delegato non possono essere aggiunti a un altro account amministratore delegato. GuardDuty Ogni organizzazione può avere un solo account GuardDuty amministratore delegato per regione e ogni account membro può avere un solo account amministratore delegato. GuardDuty

Scegli uno dei metodi di accesso per consolidare gli account GuardDuty amministratore in un unico account amministratore delegato GuardDuty .

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Per accedere, utilizza le credenziali dell'account di gestione dell'organizzazione.
2. Tutti gli account che desideri gestire GuardDuty devono far parte della tua organizzazione. Per informazioni sull'aggiunta di un account alla tua organizzazione, vedi Invitare un utente Account AWS a entrare a far parte della tua organizzazione.
3. Assicurati che tutti gli account membro siano associati all'account che desideri designare come unico account amministratore delegato GuardDuty . Disassocia qualsiasi account membro che è ancora associato agli account amministratore preesistenti.

   I seguenti passaggi sono utili per disassociare gli account membri dall'account amministratore preesistente:

   a. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
   b. Per accedere, utilizza le credenziali dell'account amministratore preesistente.
   c. Dal riquadro di navigazione, selezionare Accounts (Account).

d. Nella pagina Account, seleziona uno o più account che desideri disassociare dall'account amministratore.

e. Scegli Operazioni, quindi Disassocia account.

f. Scegli Conferma per completare il passaggio.

4. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Per accedere, utilizza le credenziali dell'account di gestione.

5. Nel pannello di navigazione scegli Impostazioni. Nella pagina Impostazioni, designa l'account GuardDuty amministratore delegato per l'organizzazione.

6. Accedere all'account amministratore delegato designato. GuardDuty

7. Aggiungi membri dall'organizzazione. Per ulteriori informazioni, consulta Gestione GuardDuty degli account con AWS Organizations.

API/CLI

1. Tutti gli account che desideri gestire GuardDuty devono far parte della tua organizzazione. Per informazioni sull'aggiunta di un account alla tua organizzazione, vedi Invitare un utente Account AWS a entrare a far parte della tua organizzazione.

2. Assicurati che tutti gli account membro siano associati all'account che desideri designare come unico account amministratore delegato GuardDuty .

   a. Esegui DisassociateMembersper dissociare qualsiasi account membro ancora associato agli account amministratore preesistenti.

   b. In alternativa, puoi usare AWS Command Line Interface per eseguire il comando seguente e sostituire *7777* con l'ID del rilevatore dell'account amministratore preesistente da cui desideri dissociare l'account membro. Sostituisci *666666666666* con l'ID Account AWS dell'account membro che desideri disassociare.

   ```
   aws guardduty disassociate-members --detector-id 777777777777 --account-
   ids 666666666666
   ```

3. Esegui EnableOrganizationAdminAccountper delegare un account Account AWS come amministratore delegato. GuardDuty

   In alternativa, puoi usare AWS Command Line Interface per eseguire il seguente comando per delegare un account amministratore delegato GuardDuty :

```
aws guardduty enable-organization-admin-account --admin-account-id 777777777777
```

4. Aggiungi membri dall'organizzazione. Per ulteriori informazioni, consulta Create or add member member accounts using API.

> **Important**
>
> Per massimizzare l'efficacia di un servizio regionale GuardDuty, ti consigliamo di designare il tuo account GuardDuty amministratore delegato e aggiungere tutti gli account membro in ogni regione.

Abilita più account GuardDuty contemporaneamente

Utilizza il seguente metodo per abilitare GuardDuty più account contemporaneamente.

Usa gli script Python per abilitare più account GuardDuty contemporaneamente

Puoi automatizzare l'attivazione o la disabilitazione di GuardDuty su più account utilizzando gli script del repository di esempio negli script multiaccount di Amazon GuardDuty . Utilizza la procedura descritta in questa sezione GuardDuty per abilitare un elenco di account membri che utilizzano Amazon EC2. Per informazioni sull'utilizzo dello script di disabilitazione o sulla configurazione dello script localmente, consulta le istruzioni contenute nel link condiviso.

Lo `enableguardduty.py` script abilita GuardDuty, invia gli inviti dall'account amministratore e accetta gli inviti in tutti gli account dei membri. Il risultato è un GuardDuty account amministratore che contiene tutti i risultati di sicurezza per tutti gli account dei membri. Poiché GuardDuty è isolato per regione, i risultati di ogni account membro vengono aggregati alla regione corrispondente nell'account amministratore. Ad esempio, la regione us-east-1 nell'account GuardDuty amministratore contiene i risultati di sicurezza per tutti i risultati us-east-1 di tutti gli account membro associati.

Questi script dipendono da un ruolo IAM condiviso con la policy gestita AWS politica gestita: AmazonGuardDutyFullAccess. Questa politica fornisce alle entità l'accesso GuardDuty e deve essere presente nell'account amministratore e in ogni account per il quale si desidera abilitare. GuardDuty

Il seguente processo è abilitato per impostazione predefinita GuardDuty in tutte le regioni disponibili. È possibile GuardDuty abilitarlo solo nelle regioni specificate utilizzando l'`--`

`enabled_regions`argomento opzionale e fornendo un elenco di regioni separate da virgole. È inoltre possibile personalizzare facoltativamente il messaggio di invito inviato agli account membri aprendo `enableguardduty.py` e modificando la stringa `gd_invite_message`.

1. Crea un ruolo IAM nell'account GuardDuty amministratore e allega la AWS politica gestita: AmazonGuardDutyFullAccess policy da abilitare. GuardDuty
2. Crea un ruolo IAM in ogni account membro che desideri venga gestito dal tuo account GuardDuty amministratore. Questo ruolo deve avere lo stesso nome del ruolo creato nella fase 1, deve consentire l'accesso all'account amministratore come entità attendibile e deve avere la stessa politica di AmazonGuardDutyFullAccess gestione descritta in precedenza.
3. Avviare una nuova istanza di Amazon Linux con un ruolo allegato che abbia la seguente relazione di trust per consentire all'istanza di assumere un ruolo di servizio.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Accedere alla nuova istanza ed eseguire i seguenti comandi per configurarla.

```
sudo yum install git python
sudo yum install python-pip
pip install boto3
aws configure
git clone https://github.com/aws-samples/amazon-guardduty-multiaccount-scripts.git
cd amazon-guardduty-multiaccount-scripts
sudo chmod +x disableguardduty.py enableguardduty.py
```

5. Creare un file CSV contenente un elenco di ID account ed e-mail degli account membri a cui è stato aggiunto un ruolo nella fase 2. Gli account devono essere visualizzati uno per riga e l'ID account e l'indirizzo di posta elettronica devono essere separati da una virgola, come nell'esempio seguente.

```
111122223333,guardduty-member@organization.com
```

> **Note**
>
> Il file CSV deve trovarsi nella stessa posizione dello script `enableguardduty.py`. È possibile copiare un file CSV esistente da Amazon S3 alla directory attuale con il seguente metodo.
>
> ```
> aws s3 cp s3://my-bucket/my_key_name example.csv
> ```

6. Eseguire lo script Python. Assicurati di fornire l'ID GuardDuty dell'account amministratore, il nome del ruolo creato nei primi passaggi e il nome del file CSV come argomenti.

```
python enableguardduty.py --master_account 444455556666 --assume_role
 roleName accountID.csv
```

Stima dei costi GuardDuty

È possibile utilizzare le operazioni della GuardDuty console o dell'API per stimare i costi di utilizzo medi giornalieri di GuardDuty. Durante il periodo di prova gratuito di 30 giorni verranno stimati i costi che si applicheranno al termine del periodo di prova. Se operi in un ambiente con più account, il tuo account GuardDuty amministratore può monitorare le metriche dei costi per tutti gli account membri.

Puoi visualizzare la stima dei costi in base alle seguenti metriche:

- ID account: elenca il costo stimato per il tuo account o per i tuoi account membro se operi come account GuardDuty amministratore.
- Origine dati: elenca il costo stimato dell'origine dati specificata per i seguenti tipi di origini GuardDuty dati: log di flusso VPC, log di CloudTrail gestione, eventi CloudTrail dati o log DNS.
- Caratteristiche: elenca il costo stimato sull'origine dati specificata per le seguenti GuardDuty funzionalità: eventi di dati per S3, EKS Audit Log Monitoring, CloudTrail dati di volume EBS, attività di accesso RDS, EKS Runtime Monitoring, Fargate Runtime Monitoring, EC2 Runtime Monitoring o Lambda Network Activity Monitoring.
- Bucket S3: elenca il costo stimato per gli eventi di dati di S3 su un bucket specifico o sui bucket più costosi per gli account nel tuo ambiente.

> **Note**
>
> Le statistiche sui bucket S3 sono disponibili solo se la Protezione S3 è abilitata per l'account. Per ulteriori informazioni, consulta Protezione Amazon S3 su Amazon GuardDuty.

Comprendere come calcola i costi di utilizzo GuardDuty

Le stime visualizzate nella GuardDuty console potrebbero differire leggermente da quelle della AWS Billing and Cost Management console. L'elenco seguente spiega come GuardDuty stimare i costi di utilizzo:

- La stima di GuardDuty utilizzo si riferisce solo alla regione corrente.
- Durante la prova gratuita di 30 giorni, la stima di GuardDuty utilizzo si basa sugli ultimi 7-30 giorni di utilizzo.

> **Note**
>
> Se la durata di utilizzo di GuardDuty o una funzionalità inclusa GuardDuty è inferiore a 7 giorni, l'importo di utilizzo viene visualizzato come ***valuta 0,00***.

- La stima dei costi di utilizzo della versione di prova include la stima relativa alle origini dati e alle funzionalità fondamentali attualmente nel periodo di prova. Ogni funzionalità e fonte di dati GuardDuty inclusa ha il proprio periodo di prova, ma può sovrapporsi al periodo di prova di GuardDuty o a un'altra funzionalità abilitata contemporaneamente.
- La stima di GuardDuty utilizzo include sconti sui prezzi per GuardDuty volume per regione, come indicato nella pagina GuardDuty dei prezzi di Amazon, ma solo per i singoli account che soddisfano i livelli di prezzo basati sui volumi. Gli sconti sui prezzi per volume non sono inclusi nelle stime relative all'utilizzo totale combinato tra gli account di un'organizzazione. Per informazioni sui prezzi scontati per volume di utilizzo combinato, consulta Fatturazione AWS : sconti per volume.

Monitoraggio del runtime: in che modo i log di flusso VPC delle istanze EC2 influiscono sui costi di utilizzo

Quando gestisci l'agente di sicurezza (manualmente o tramite GuardDuty) in EKS Runtime Monitoring o Runtime Monitoring for EC2 e GuardDuty viene attualmente distribuito su un'istanza Amazon EC2 e riceve i dati Tipi di eventi di runtime raccolti da questa istanza, non GuardDuty ti verrà addebitato alcun costo per Account AWS l'analisi dei log di flusso VPC da questa istanza Amazon EC2. Questo aiuta a GuardDuty evitare il doppio dei costi di utilizzo dell'account.

Come GuardDuty stima i costi di utilizzo per CloudTrail gli eventi

Quando lo abiliti GuardDuty, inizia automaticamente a consumare i registri degli AWS CloudTrail eventi registrati per il tuo account nel gruppo selezionato Regione AWS. GuardDuty replica i registri degli eventi del servizio globale e quindi elabora questi eventi in modo indipendente in ogni regione in cui è stata abilitata. GuardDuty Questo aiuta a GuardDuty mantenere i profili utente e di ruolo in ogni regione per identificare le anomalie.

La CloudTrail configurazione non influisce sui costi di GuardDuty utilizzo o sul modo in cui GuardDuty elabora i registri degli eventi. Il costo di GuardDuty utilizzo è influenzato dall'utilizzo delle AWS API a cui si accede. CloudTrail Per ulteriori informazioni, consulta AWS CloudTrail registri degli eventi.

Revisione delle statistiche GuardDuty di utilizzo

Scegli il tuo metodo di accesso preferito per rivedere le statistiche di utilizzo del tuo GuardDuty account. Se sei un account GuardDuty amministratore, i seguenti metodi ti aiuteranno a rivedere le statistiche di utilizzo per tutti i membri.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare l'account GuardDuty amministratore.
2. Nel riquadro di navigazione, scegli Utilizzo.
3. Nella pagina Utilizzo, un account GuardDuty amministratore con account membro può visualizzare il costo stimato dell'organizzazione per gli ultimi 30 giorni. Si tratta di un costo di utilizzo totale stimato per l'organizzazione.
4. GuardDuty gli account amministratore con membri possono visualizzare la ripartizione dei costi di utilizzo per origine dati o per account. Gli account individuali o autonomi possono visualizzare la suddivisione per fonte di dati.

   Se disponi di account membri, puoi visualizzare le statistiche di un singolo account selezionando tale account nella tabella Conti.

API/CLI

Esegui l'operazione GetUsageStatisticsAPI utilizzando le credenziali dell'account GuardDuty amministratore. Fornisci le seguenti informazioni per eseguire il comando:

- (Obbligatorio) Fornisci l'ID del GuardDuty rilevatore regionale dell'account per il quale desideri recuperare le statistiche.
- (Obbligatorio) fornisci uno dei tipi di statistiche da recuperare: `SUM_BY_ACCOUNT | SUM_BY_DATA_SOURCE | SUM_BY_RESOURCE | SUM_BY_FEATURE | TOP_ACCOUNTS_BY_FEATURE`.

  Attualmente, `TOP_ACCOUNTS_BY_FEATURE` non supporta il recupero delle statistiche di utilizzo per. `RDS_LOGIN_EVENTS`
- (Obbligatorio) Fornisci una o più fonti di dati o funzionalità per interrogare le tue statistiche di utilizzo.

- (Facoltativo) fornisci un elenco di ID account per i quali desideri recuperare le statistiche di utilizzo.

Puoi anche utilizzare l' AWS Command Line Interface. Il comando seguente è un esempio di recupero delle statistiche di utilizzo per tutte le fonti di dati e le funzionalità, calcolate dagli account. Assicurati di sostituire il `detector-id` con il tuo ID rilevatore valido. Per gli account autonomi, questo comando restituisce il costo di utilizzo degli ultimi 30 giorni relativi solo al proprio account. Se sei un account GuardDuty amministratore con account membri, vedrai i costi elencati per account per tutti i membri.

Per trovare i dati `detectorId` relativi al tuo account e alla regione corrente, consulta la pagina Impostazioni nella console https://console.aws.amazon.com/guardduty/.

Sostituisci `SUM_BY_ACCOUNT` con il tipo con cui desideri calcolare le statistiche di utilizzo.

Per monitorare i costi solo per le fonti di dati

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"DataSources":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_LOGS", "KUBERNETES_AUDIT_LOGS",
 "EC2_MALWARE_SCAN"]}'
```

Per monitorare i costi delle funzionalità

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"Features":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_DATA_EVENTS", "EKS_AUDIT_LOGS",
 "EBS_MALWARE_PROTECTION", "RDS_LOGIN_EVENTS", "LAMBDA_NETWORK_LOGS",
 "EKS_RUNTIME_MONITORING", "FARGATE_RUNTIME_MONITORING", "EC2_RUNTIME_MONITORING"]}'
```

Sicurezza in Amazon GuardDuty

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, è possibile trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra te e AWS. Il Modello di responsabilità condivisa descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS nel cloud AWS. AWS fornisce inoltre servizi che puoi utilizzare in sicurezza. Gli auditor di terze parti testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei programmi di conformità AWS. Per avere maggiori informazioni sui programmi di conformità applicabili a GuardDuty, consulta Servizi AWS rientranti nell'ambito del programma di conformità.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi. Inoltre, sei responsabile anche di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione consente di comprendere come applicare il modello di responsabilità condivisa durante l'utilizzo di GuardDuty. Viene illustrato come configurare GuardDuty per soddisfare gli obiettivi di sicurezza e conformità. Scoprirai anche come utilizzare altri servizi AWS per monitorare e proteggere le risorse GuardDuty.

Indice

- Protezione dei dati in Amazon GuardDuty
- Registrazione delle chiamate GuardDuty API Amazon con AWS CloudTrail
- Identity and Access Management per Amazon GuardDuty
- Convalida della conformità per Amazon GuardDuty
- Resilienza in Amazon GuardDuty
- Sicurezza dell'infrastruttura in Amazon GuardDuty

Protezione dei dati in Amazon GuardDuty

Il modello di responsabilità AWS condivisa di si applica alla protezione dei dati in Amazon GuardDuty. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale

che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori o Servizi AWS utilizzi la console, l'API GuardDuty o gli SDK. AWS CLI AWS I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati a riposo

Tutti i dati dei GuardDuty clienti vengono crittografati quando sono inattivi utilizzando soluzioni di AWS crittografia.

GuardDuty i dati, come i risultati, vengono crittografati quando sono inattivi utilizzando AWS Key Management Service (AWS KMS) utilizzando chiavi gestite dal cliente di AWS proprietà.

Crittografia in transito

GuardDuty analizza i dati di registro di altri servizi. e crittografa tutti i dati in transito con HTTPS e KMS. Una volta GuardDuty estratte le informazioni necessarie dai log, queste vengono eliminate. Per ulteriori informazioni su come GuardDuty utilizza le informazioni di altri servizi, consulta le fonti di dati. GuardDuty

GuardDuty i dati vengono crittografati durante il transito tra i servizi.

Rifiuto esplicito all'utilizzo dei dati volto al miglioramento del servizio

Puoi scegliere di non utilizzare i tuoi dati per sviluppare GuardDuty e migliorare altri servizi di AWS sicurezza utilizzando la politica di AWS Organizations opt-out. Puoi scegliere di rinunciare anche se al momento GuardDuty non raccoglie tali dati. Per ulteriori informazioni in merito, consulta le Policy di rifiuto dei servizi di IA nella Guida per l'utente di AWS Organizations .

> **Note**
>
> Per poter utilizzare la politica di opt-out, i tuoi AWS account devono essere gestiti centralmente da AWS Organizations. Se non hai ancora creato un'organizzazione per i tuoi AWS account, consulta Creazione e gestione di un'organizzazione nella Guida per l'AWS Organizations utente.

Il rifiuto esplicito ha gli effetti seguenti:

- GuardDuty eliminerà i dati raccolti e archiviati per scopi di miglioramento del servizio prima dell'eventuale rinuncia da parte dell'utente.
- Dopo l'annullamento, non GuardDuty raccoglieremo o memorizzeremo più questi dati per scopi di miglioramento del servizio.

I seguenti argomenti spiegano come ciascuna funzionalità all'interno di ciascuna funzionalità gestisca GuardDuty potenzialmente i dati per il miglioramento del servizio.

Indice

- GuardDuty Monitoraggio del runtime
- GuardDuty Protezione da malware

GuardDuty Monitoraggio del runtime

GuardDuty Il monitoraggio del runtime fornisce il rilevamento delle minacce in fase di esecuzione solo per i cluster Amazon Elastic Kubernetes Service (Amazon EKS) AWS Fargate (Fargate) , Amazon Elastic Container Service (Amazon ECS) e le istanze Amazon Elastic Compute Cloud (Amazon EC2) nel tuo ambiente. AWS Dopo aver abilitato il Runtime Monitoring e distribuito l'agente di GuardDuty sicurezza per la tua risorsa, GuardDuty inizia a monitorare e analizzare gli eventi di runtime associati alla tua risorsa. Questi tipi di eventi di runtime includono eventi di processo, eventi container, eventi DNS e altro ancora. Per ulteriori informazioni, consulta Tipi di eventi di runtime raccolti che utilizza GuardDuty .

Sebbene GuardDuty ora raccolga argomenti della riga di comando che puoi indirizzare ai tuoi carichi di lavoro, attualmente non utilizza questi argomenti per scopi di miglioramento del servizio (potrebbe farlo in futuro). Abbiamo iniziato a raccogliere argomenti da riga di comando in previsione delle nuove regole e dei risultati di rilevamento delle minacce che verranno rilasciati a breve. La tua fiducia, la tua privacy e la sicurezza dei tuoi contenuti sono la nostra massima priorità e garantiamo che il nostro utilizzo rispetta i nostri impegni nei tuoi confronti. Per ulteriori informazioni, consulta le Domande frequenti sulla privacy dei dati in .

GuardDuty Protezione da malware

GuardDuty Malware Protection analizza e rileva il malware contenuto nei volumi EBS collegati ai carichi di lavoro di istanze Amazon EC2 e container potenzialmente compromessi. Quando GuardDuty Malware Protection identifica un file di volume EBS come dannoso o dannoso, GuardDuty Malware Protection raccoglie e archivia questo file per sviluppare e migliorare i rilevamenti di malware e il servizio. GuardDuty Questo file può essere utilizzato anche per sviluppare e migliorare altri servizi di sicurezza. AWS La tua fiducia, la tua privacy e la sicurezza dei tuoi contenuti sono la nostra massima priorità e garantiamo che il nostro utilizzo rispetta i nostri impegni nei tuoi confronti. Per ulteriori informazioni, consulta le Domande frequenti sulla privacy dei dati in .

Registrazione delle chiamate GuardDuty API Amazon con AWS CloudTrail

Amazon GuardDuty è integrato conAWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in GuardDuty. CloudTrail acquisisce tutte le chiamate API relative GuardDuty agli eventi, incluse le chiamate dalla GuardDuty console e le chiamate in codice alle GuardDuty API. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi

a un bucket Amazon Simple Storage Service (Amazon S3), inclusi gli eventi per. GuardDuty Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta a cui è stata effettuata GuardDuty, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, incluse le modalità di configurazione e attivazione, consulta la Guida per l'AWS CloudTrailutente.

GuardDuty informazioni in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività di evento supportata in GuardDuty, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi di GuardDuty, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le Regioni . Il trail registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consultare:

- Panoramica della creazione di un percorso
- Servizi e integrazioni CloudTrail supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali di accesso utente root o utente IAM
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail .

GuardDuty eventi del piano di controllo in CloudTrail

Per impostazione predefinita, CloudTrail registra tutte le operazioni GuardDuty API fornite in Amazon GuardDuty API Reference come eventi nei CloudTrail file.

GuardDuty eventi relativi ai dati in CloudTrail

GuardDuty Monitoraggio del runtimeutilizza un agente di GuardDuty sicurezza distribuito nei cluster Amazon Elastic Kubernetes Service (Amazon EKS), solo nelle attività Amazon Elastic Compute Cloud (Amazon EC2) e nelle `aws-guardduty-agent` attività (Amazon Elastic Container Service (AWS FargateAmazon ECS)) per raccogliere componenti aggiuntivi () che raccolgono Tipi di eventi di runtime raccolti i carichi di lavoro e inviarli a rilevamento e analisi delle minacce. AWS GuardDuty

Registrazione e monitoraggio degli eventi di dati

Facoltativamente, puoi configurare i log per visualizzare gli eventi relativi ai dati per il tuo agente di sicurezza. AWS CloudTrail GuardDuty

Per creare e configurare CloudTrail, consulta Data events nella Guida per l'AWS CloudTrailutente e segui le istruzioni per Logging data events con selettori di eventi avanzati in. AWS Management Console Durante la registrazione del trail, assicurati di apportare le modifiche seguenti:

- Per il tipo di evento Data, scegli GuardDuty detector.
- Per il Modello di selettore di log, scegli Registra tutti gli eventi.
- Espandi la Visualizzazione JSON per la configurazione, che dovrebbe essere simile al file JSON seguente:

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
```

```
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

Dopo aver abilitato il selettore per il percorso, accedi alla console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/. Puoi scaricare gli eventi relativi ai dati dal bucket S3 scelto al momento della configurazione dei log. CloudTrail

Esempio: voci dei file di registro GuardDuty

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che mostra l'evento del piano dati.

```
{
        "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"
        }
    }
```


L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'`CreateIPThreatIntelSet`azione (evento del piano di controllo).


```
{
    "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"
}
```


Da queste informazioni sull'evento puoi determinare che la richiesta è stata effettuata per creare un elenco di minacce `Example` in GuardDuty. Puoi inoltre vedere che la richiesta è stata effettuata da un utente denominato Alice il 14 giugno 2018.

Identity and Access Management per Amazon GuardDuty

AWS Identity and Access Management (IAM) è un Servizio AWS che consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. GuardDuty IAM è un Servizio AWS il cui uso non comporta costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Come GuardDuty funziona Amazon con IAM
- Esempi di policy basate sull'identità per Amazon GuardDuty
- Utilizzo di ruoli collegati ai servizi per Amazon GuardDuty
- Risoluzione dei problemi relativi all' GuardDuty identità e all'accesso ad Amazon
- AWS politiche gestite per Amazon GuardDuty

Destinatari

Le modalità di utilizzo di AWS Identity and Access Management (IAM) cambiano in base alle operazioni eseguite in GuardDuty.

Utente del servizio: se utilizzi il GuardDuty servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più GuardDuty funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di GuardDuty, consulta Risoluzione dei problemi relativi all' GuardDuty identità e all'accesso ad Amazon.

Amministratore del servizio: se sei responsabile delle GuardDuty risorse della tua azienda, probabilmente hai pieno accesso a GuardDuty. È tuo compito determinare a quali GuardDuty funzionalità e risorse devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su

come la tua azienda può utilizzare IAM con GuardDuty, consultaCome GuardDuty funziona Amazon con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a GuardDuty. Per visualizzare esempi di policy GuardDuty basate sull'identità che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità per Amazon GuardDuty

Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWS con le credenziali di identità. Devi essere autenticato (connesso a AWS) come utente root Utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

Puoi accedere ad AWS come identità federata utilizzando le credenziali fornite attraverso un'origine di identità. AWS IAM Identity Center Gli esempi di identità federate comprendono gli utenti del centro identità IAM, l'autenticazione Single Sign-On (SSO) dell'azienda e le credenziali di Google o Facebook. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Se accedi ad AWS tramite la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere alla AWS Management Console o al portale di accesso AWS. Per ulteriori informazioni sull'accesso ad AWS, consulta la sezione Come accedere al tuo Account AWS nella Guida per l'utente di Accedi ad AWS.

Se accedi ad AWS in modo programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia della linea di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sulla firma delle richieste, consultare Firma delle richieste AWS nella Guida per l'utente di IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza dell'account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWS e le risorse nell'account. Tale identità è detta utente root Account AWS ed è possibile accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Tasks that require root user credentials (Attività che richiedono le credenziali dell'utente root) nella Guida per l'utente di IAM.

Identità federata

Come best practice, richiedere agli utenti umani, compresi quelli che richiedono l'accesso di amministratore, di utilizzare la federazione con un provider di identità per accedere a Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory degli utenti aziendali, un provider di identità Web, AWS Directory Service, la directory Identity Center o qualsiasi utente che accede ad Servizi AWS utilizzando le credenziali fornite tramite un'origine di identità. Quando le identità federate accedono ad Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un gruppo di utenti e gruppi nell'origine di identità per utilizzarli in tutte le applicazioni e gli Account AWS. Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center.

Utenti e gruppi IAM

Un utente IAM è una identità all'interno del tuo Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla

volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità all'interno di Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM nella AWS Management Console mediante lo scambio di ruoli. È possibile assumere un ruolo chiamando un'operazione AWS CLI o API AWS oppure utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center.
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, per alcuni dei Servizi AWS, è possibile collegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

- Accesso multi-servizio: alcuni Servizi AWS utilizzano funzionalità che in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Inoltro delle sessioni di accesso (FAS): quando utilizzi un ruolo o un utente IAM per eseguire azioni in AWS, sei considerato un principale. Quando utilizzi alcuni servizi, puoi eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altre risorse o Servizi AWS per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Inoltro sessioni di accesso.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLI o dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo dell'istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Per controllare l'accesso a AWS è possibile creare policy e collegarle a identità o risorse AWS. Una policy è un oggetto in AWS che, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste policy quando un principale IAM (utente, utente root o sessione ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWS sotto forma di documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare l'accesso ai diversi elementi. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dalla AWS Management Console, la AWS CLI o l'API AWS.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWS e le policy gestite dal cliente. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di trust dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy gestite da AWS da IAM in una policy basata su risorse.

Liste di controllo accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3, AWS WAF e Amazon VPC sono esempi di servizi che supportano le ACL. Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta altri tipi di policy meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Policy di controllo dei servizi (SCP): le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata degli Account AWS

multipli di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni Utente root dell'account AWS. Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations.

- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella Guida per l'utente di IAM.

Come GuardDuty funziona Amazon con IAM

Prima di utilizzare IAM per gestire l'accesso a GuardDuty, scopri con quali funzionalità IAM è disponibile l'uso GuardDuty.

Funzionalità IAM che puoi utilizzare con Amazon GuardDuty

Funzionalità IAM	GuardDuty supporto
Policy basate su identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì

Funzionalità IAM	GuardDuty supporto
Liste di controllo degli accessi	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

Per avere una panoramica di alto livello su come GuardDuty e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWSi servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per GuardDuty

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o rifiutate, nonché le condizioni in base alle quali le operazioni sono consentite o rifiutate. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di politiche basate sull'identità per GuardDuty

Per visualizzare esempi di politiche basate sull' GuardDuty identità, vedere. Esempi di policy basate sull'identità per Amazon GuardDuty

Politiche basate sulle risorse all'interno GuardDuty

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di trust dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata su risorse rappresenta solo una parte della relazione di attendibilità. Quando l'entità principale e la risorsa si trovano in diversi Account AWS, un amministratore IAM nell'account attendibile deve concedere all'entità principale (utente o ruolo) anche l'autorizzazione per accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Azioni politiche per GuardDuty

Supporta le azioni di policy	Sì

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni di policy hanno spesso lo stesso nome dell'operazione API AWS. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più azioni in una policy. Queste azioni aggiuntive sono denominate azioni dipendenti.

Includi le azioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di GuardDuty azioni, consulta Azioni definite da Amazon GuardDuty nel Service Authorization Reference.

Le azioni politiche in GuardDuty uso utilizzano il seguente prefisso prima dell'azione:

```
guardduty
```

Per specificare più azioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "guardduty:action1",
      "guardduty:action2"
         ]
```

Per visualizzare esempi di politiche GuardDuty basate sull'identità, vedere. Esempi di policy basate sull'identità per Amazon GuardDuty

Risorse politiche per GuardDuty

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di GuardDuty risorse e dei relativi ARN, consulta Resources defined by Amazon GuardDuty nel Service Authorization Reference. Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, consulta Azioni definite da Amazon. GuardDuty

Per visualizzare esempi di politiche GuardDuty basate sull'identità, consulta. Esempi di policy basate sull'identità per Amazon GuardDuty

Chiavi relative alle condizioni delle politiche per GuardDuty

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se specifichi più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione `OR` logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

Per visualizzare un elenco di chiavi di GuardDuty condizione, consulta Condition keys for Amazon GuardDuty nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Azioni definite da Amazon GuardDuty.

Per visualizzare esempi di politiche GuardDuty basate sull'identità, consulta. Esempi di policy basate sull'identità per Amazon GuardDuty

Liste di controllo degli accessi (ACL) in GuardDuty

Supporta le ACL	No

Le policy di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Controllo degli accessi basato sugli attributi (ABAC) con GuardDuty

Supporta ABAC (tag nelle policy)	Parziale

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, tali attributi sono denominati tag. È possibile collegare dei tag alle entità IAM (utenti o ruoli) e a numerose risorse AWS. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Partial (Parziale).

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con le fasi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con GuardDuty

Supporta le credenziali temporanee	Sì

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi i Servizi AWS che funzionano con le credenziali temporanee, consulta Servizi AWS supportati da IAM nella Guida per l'utente di IAM.

Le credenziali temporanee sono utilizzate se si accede alla AWS Management Console utilizzando qualsiasi metodo che non sia la combinazione di nome utente e password. Ad esempio, quando accedi alla AWS utilizzando il collegamento Single Sign-On (SSO) della tua azienda, tale processo crea in automatico credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando la AWS CLI o l'API AWS. È quindi possibile utilizzare tali credenziali temporanee per accedere ad AWS. AWS consiglia di generare le credenziali temporanee dinamicamente anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni principali multiservizio per GuardDuty

Supporta l'inoltro delle sessioni di accesso (FAS)	Sì

Quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un'entità principale. Quando utilizzi alcuni servizi, puoi eseguire un'operazione che attiva un'altra operazione in un servizio differente. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altre risorse o Servizi AWS per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Inoltro sessioni di accesso.

Ruoli di servizio per GuardDuty

Supporta i ruoli di servizio	Sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per

ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità. GuardDuty Modifica i ruoli di servizio solo quando viene GuardDuty fornita una guida in tal senso.

Ruoli collegati ai servizi per GuardDuty

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato ai servizi è un tipo di ruolo di servizio che è collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione di ruoli GuardDuty collegati ai servizi, vedere. Utilizzo di ruoli collegati ai servizi per Amazon GuardDuty

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per Amazon GuardDuty

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse GuardDuty. Inoltre, non sono in grado di eseguire attività utilizzando la AWS Management Console, l'AWS Command Line Interface (AWS CLI) o l'API AWS. Per concedere agli utenti l'autorizzazione per eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da GuardDuty, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon GuardDuty nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console di GuardDuty
- Autorizzazioni necessarie per abilitare GuardDuty
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Policy IAM personalizzata per concedere l'accesso in sola lettura a GuardDuty
- Negare l'accesso ai risultati GuardDuty
- Utilizzo di una policy IAM personalizzata per limitare l'accesso alle GuardDuty risorse

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare GuardDuty risorse nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Nozioni di base sulle policy gestite da AWS e passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWS che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWS specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate

utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console di GuardDuty

Per accedere alla GuardDuty console Amazon, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle GuardDuty risorse del tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario che concedi le autorizzazioni minime della console agli utenti che effettuano chiamate solo alla AWS CLI o all'API AWS. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che gli utenti e i ruoli possano ancora utilizzare la GuardDuty console, allega anche la policy GuardDuty `ConsoleAccess` o la policy `ReadOnly` AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Autorizzazioni necessarie per abilitare GuardDuty

Per concedere le autorizzazioni necessarie a diverse identità IAM (utenti, gruppi e ruoli), allega la AWS politica gestita: AmazonGuardDutyFullAccess policy di attivazione richiesta. GuardDuty

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono allegate alla relativa identità utente. La policy include le autorizzazioni per completare questa azione sulla console o a livello di programmazione utilizzando la AWS CLI o l'API 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": "*"
        }
    ]
}
```

Policy IAM personalizzata per concedere l'accesso in sola lettura a GuardDuty

Per concedere l'accesso in sola lettura GuardDuty puoi utilizzare la policy gestita. `AmazonGuardDutyReadOnlyAccess`

Per creare una policy personalizzata che conceda l'accesso in sola lettura a un ruolo, un utente o un gruppo IAM GuardDuty, puoi utilizzare la seguente dichiarazione:

```
{
    "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": "*"
        }
    ]
}
```

Negare l'accesso ai risultati GuardDuty

Puoi utilizzare la seguente policy per negare a un ruolo, utente o gruppo IAM l'accesso ai GuardDuty risultati. Gli utenti non possono visualizzare i risultati o i dettagli sui risultati, ma possono accedere a tutte le altre GuardDuty operazioni:

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

Utilizzo di una policy IAM personalizzata per limitare l'accesso alle GuardDuty risorse

Per definire l'accesso di un utente in GuardDuty base all'ID del rilevatore, puoi utilizzare tutte le azioni GuardDuty API nelle tue policy IAM personalizzate, ad eccezione delle seguenti operazioni:

- `guardduty:CreateDetector`
- `guardduty:DeclineInvitations`
- `guardduty:DeleteInvitations`
- `guardduty:GetInvitationsCount`
- `guardduty:ListDetectors`
- `guardduty:ListInvitations`

Utilizza le seguenti operazioni in una policy IAM per definire l'accesso di un utente a in GuardDuty base all'ID e ThreatIntelSet all'ID IPSet:

- `guardduty:DeleteIPSet`

- `guardduty:DeleteThreatIntelSet`
- `guardduty:GetIPSet`
- `guardduty:GetThreatIntelSet`
- `guardduty:UpdateIPSet`
- `guardduty:UpdateThreatIntelSet`

I seguenti esempi mostrano come creare delle policy utilizzando alcune delle operazioni precedenti:

- Questa policy consente a un utente di eseguire l'operazione `guardduty:UpdateDetector` utilizzando l'ID rilevatore 1234567 nella regione us-east-1:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateDetector",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567"
        }
    ]
}
```

- Questa policy consente a un utente di eseguire l'operazione `guardduty:UpdateIPSet` utilizzando l'ID rilevatore 1234567 e l'ID IPSet 000000 nella regione us-east-1:

> **Note**
>
> Assicurati che l'utente disponga delle autorizzazioni necessarie per accedere agli elenchi di IP affidabili e agli elenchi di minacce in. GuardDuty Per ulteriori informazioni, consulta Autorizzazioni necessarie per caricare elenchi di indirizzi IP affidabili ed elenchi minacce.

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

```
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/000000"
        }
    ]
}
```

- Questa policy consente a un utente di eseguire l'operazione `guardduty:UpdateIPSet` utilizzando qualsiasi ID rilevatore e l'ID IPSet 000000 nella regione us-east-1:

> **Note**
>
> Assicurati che l'utente disponga delle autorizzazioni necessarie per accedere agli elenchi di IP affidabili e agli elenchi di minacce in. GuardDuty Per ulteriori informazioni, consulta Autorizzazioni necessarie per caricare elenchi di indirizzi IP affidabili ed elenchi minacce.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
        }
    ]
}
```

- Questa policy consente a un utente di eseguire l'operazione `guardduty:UpdateIPSet` utilizzando il proprio ID rilevatore e qualsiasi ID IPSet nella regione us-east-1:

> **Note**
>
> Assicurati che l'utente disponga delle autorizzazioni necessarie per accedere agli elenchi di IP affidabili e agli elenchi di minacce in. GuardDuty Per ulteriori informazioni, consulta Autorizzazioni necessarie per caricare elenchi di indirizzi IP affidabili ed elenchi minacce.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/*"
        }
    ]
}
```

Utilizzo di ruoli collegati ai servizi per Amazon GuardDuty

Amazon GuardDuty utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato al servizio (SLR) è un tipo unico di ruolo IAM a cui è collegato direttamente. GuardDuty I ruoli collegati ai servizi sono predefiniti GuardDuty e includono tutte le autorizzazioni necessarie per chiamare altri servizi per GuardDuty tuo conto. AWS

Con il ruolo collegato al servizio, puoi eseguire la configurazione GuardDuty senza aggiungere manualmente le autorizzazioni necessarie. GuardDuty definisce le autorizzazioni del suo ruolo collegato al servizio e, a meno che le autorizzazioni non siano definite diversamente, solo può assumere il ruolo. GuardDuty Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

GuardDuty supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui è disponibile. GuardDuty Per ulteriori informazioni, consulta Regioni ed endpoint.

È possibile eliminare il ruolo GuardDuty collegato al servizio solo dopo la prima disabilitazione GuardDuty in tutte le regioni in cui è abilitato. In questo modo proteggi GuardDuty le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedervi.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta Servizi AWS che funzionano con IAM nella Guida per l'utente IAM e cerca i servizi che riportano Sì nella colonna Ruoli collegati al servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate al servizio per GuardDuty

GuardDuty utilizza il ruolo collegato al servizio (SLR) denominato. `AWSServiceRoleForAmazonGuardDuty` La SLR consente di GuardDuty eseguire le seguenti attività. Consente inoltre di GuardDuty includere i metadati recuperati appartenenti all'istanza EC2 nei risultati che GuardDuty possono generare sulla potenziale minaccia. Ai fini dell'assunzione del ruolo `AWSServiceRoleForAmazonGuardDuty`, il ruolo collegato ai servizi `guardduty.amazonaws.com`considera attendibile il servizio.

Le politiche di autorizzazione aiutano a GuardDuty svolgere le seguenti attività:

- Utilizzare le operazioni di Amazon EC2 per gestire e recuperare informazioni su istanze EC2, immagini e componenti di rete come VPC, sottoreti, gateway di transito e gruppi di sicurezza.
- Usa AWS Systems Manager le azioni per gestire le associazioni SSM sulle istanze Amazon EC2 quando GuardDuty abiliti il monitoraggio del runtime con agente automatizzato per Amazon EC2. Quando la configurazione GuardDuty automatizzata degli agenti è disabilitata, GuardDuty considera solo le istanze EC2 che hanno un tag di inclusione (:). `GuardDutyManaged true`
- Utilizza AWS Organizations le azioni per descrivere gli account e l'ID dell'organizzazione associati.
- Utilizzare le operazioni di Amazon S3 per recuperare informazioni su bucket e oggetti S3.
- Usa AWS Lambda le azioni per recuperare informazioni sulle funzioni e sui tag Lambda.
- Utilizzare le operazioni di Amazon EKS per gestire e recuperare informazioni sui cluster EKS e gestire i Componenti aggiuntivi di Amazon EKS su questi cluster. Le azioni EKS recuperano anche le informazioni sui tag associati a. GuardDuty
- Utilizzare IAM per creare una Autorizzazioni del ruolo collegato ai servizi per la protezione da malware dopo che la protezione da malware è stata abilitata.
- Utilizza le azioni Amazon ECS per gestire e recuperare informazioni sui cluster Amazon ECS e gestisci le impostazioni dell'account Amazon ECS con. `guarddutyActivate` Le azioni relative ad Amazon ECS recuperano anche le informazioni sui tag associati a. GuardDuty

Il ruolo è configurato con le seguenti policy gestite da AWS, denominate `AmazonGuardDutyServiceRolePolicy`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GuardDutyGetDescribeListPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeTransitGatewayAttachments",
                "organizations:ListAccounts",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketTagging",
                "s3:GetAccountPublicAccessBlock",
                "s3:ListAllMyBuckets",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "lambda:GetFunctionConfiguration",
                "lambda:ListTags",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeSecurityGroups",
                "ecs:ListClusters",
                "ecs:DescribeClusters"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GuardDutyCreateSLRPolicy",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                },
                "StringLike": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.*.guardduty-data",
                        "com.amazonaws.*.guardduty-data-fips"
                    ]
                }
            }
        },
        {
            "Sid": "GuardDutyModifyDeleteVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpoint",
                "ec2:DeleteVpcEndpoints"
            ],
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpoint",
                "ec2:ModifyVpcEndpoint"
            ],
```

```
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*",
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:subnet/*"
            ]
        },
        {
             "Sid": "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
             "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateVpcEndpoint"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutySecurityGroupManagementPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringLike": {
```

```
                "aws:RequestTag/GuardDutyManaged": "*"
            }
        }
    },
    {
        "Sid": "GuardDutyCreateSecurityGroupForVpcPolicy",
        "Effect": "Allow",
        "Action": "ec2:CreateSecurityGroup",
        "Resource": "arn:aws:ec2:*:*:vpc/*"
    },
    {
        "Sid": "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
        "Effect": "Allow",
        "Action": "ec2:CreateTags",
        "Resource": "arn:aws:ec2:*:*:security-group/*",
        "Condition": {
            "StringEquals": {
                "ec2:CreateAction": "CreateSecurityGroup"
            },
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": "GuardDutyManaged"
            }
        }
    },
    {
        "Sid": "GuardDutyCreateEksAddonPolicy",
        "Effect": "Allow",
        "Action": "eks:CreateAddon",
        "Resource": "arn:aws:eks:*:*:cluster/*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": "GuardDutyManaged"
            }
        }
    },
    {
        "Sid": "GuardDutyEksAddonManagementPolicy",
        "Effect": "Allow",
        "Action": [
            "eks:DeleteAddon",
            "eks:UpdateAddon",
            "eks:DescribeAddon"
        ],
        "Resource": "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
```

```
        },
        {
            "Sid": "GuardDutyEksClusterTagResourcePolicy",
            "Effect": "Allow",
            "Action": "eks:TagResource",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEcsPutAccountSettingsDefaultPolicy",
            "Effect": "Allow",
            "Action": "ecs:PutAccountSettingDefault",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecs:account-setting": [
                        "guardDutyActivate"
                    ]
                 }
            }
        },
        {
            "Sid": "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeAssociation",
                "ssm:DeleteAssociation",
                "ssm:UpdateAssociation",
                "ssm:CreateAssociation",
                "ssm:StartAssociationsOnce"
            ],
            "Resource": "arn:aws:ssm:*:*:association/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
        },
        {
            "Sid": "SsmAddTagsToResourcePermission",
```

```
            "Effect": "Allow",
            "Action": [
                "ssm:AddTagsToResource"
            ],
            "Resource": "arn:aws:ssm:*:*:association/*",
            "Condition":{
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                },
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
        },
        {
            "Sid": "SsmCreateUpdateAssociationInstanceDocumentPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateAssociation",
                "ssm:UpdateAssociation"
            ],
            "Resource": "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
        },
        {
            "Sid": "SsmSendCommandPermission",
            "Effect": "Allow",
            "Action": "ssm:SendCommand",
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
            ]
        },
        {
            "Sid": "SsmGetCommandStatus",
            "Effect": "Allow",
            "Action": "ssm:GetCommandInvocation",
            "Resource": "*"
        }
    ]
```

```
}
```

Di seguito è riportata la policy di attendibilità associata al ruolo collegato ai servizi `AWSServiceRoleForAmazonGuardDuty`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Creazione di un ruolo collegato al servizio per GuardDuty

Il ruolo `AWSServiceRoleForAmazonGuardDuty` collegato al servizio viene creato automaticamente quando lo si abilita GuardDuty per la prima volta o si abilita GuardDuty in una regione supportata in cui in precedenza non era abilitato. Puoi anche creare il ruolo collegato al servizio manualmente utilizzando la console IAM, l'o l'API AWS CLI IAM.

> **Important**
>
> Il ruolo collegato al servizio creato per l'account amministratore GuardDuty delegato non si applica agli account dei membri. GuardDuty

Per consentire a un principale IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. `AWSServiceRoleForAmazonGuardDuty`Affinché il ruolo collegato al servizio venga creato correttamente, il principale IAM con cui lo utilizzi deve disporre delle autorizzazioni GuardDuty richieste. Per concedere le autorizzazioni richieste, collega la seguente policy gestita a questo utente, gruppo o ruolo .

> **Note**
>
> Sostituisci l'*ID dell'account* di esempio nell'esempio seguente con l'ID dell'account effettivo AWS .

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

Per ulteriori informazioni sulla creazione manuale del ruolo, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente IAM.

Modifica di un ruolo collegato al servizio per GuardDuty

GuardDuty non consente di modificare il ruolo collegato al `AWSServiceRoleForAmazonGuardDuty` servizio. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per GuardDuty

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non hai un'entità non utilizzata che non viene monitorata o gestita attivamente.

> **Important**
>
> Se hai abilitato la protezione da malware, l'eliminazione del `AWSServiceRoleForAmazonGuardDuty` non comporta l'eliminazione automatica del `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Se desideri eliminare il `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, consulta Eliminazione di un ruolo collegato ai servizi per la protezione da malware.

È necessario innanzitutto disabilitarlo GuardDuty in tutte le regioni in cui è abilitato per eliminare il. `AWSServiceRoleForAmazonGuardDuty` Se il GuardDuty servizio non è disabilitato quando si tenta di eliminare il ruolo collegato al servizio, l'eliminazione non riesce. Per ulteriori informazioni, consulta Sospensione o disabilitazione GuardDuty.

Quando si disattiva GuardDuty, `AWSServiceRoleForAmazonGuardDuty` non viene eliminato automaticamente. Se lo abiliti GuardDuty nuovamente, inizierà a utilizzare l'esistente`AWSServiceRoleForAmazonGuardDuty`.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l'API IAM per eliminare il ruolo `AWSServiceRoleForAmazonGuardDuty` collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Supportato Regioni AWS

Amazon GuardDuty supporta l'utilizzo del ruolo `AWSServiceRoleForAmazonGuardDuty` collegato al servizio Regioni AWS ovunque GuardDuty sia disponibile. Per un elenco delle regioni in cui GuardDuty è attualmente disponibile, consulta gli GuardDuty endpoint e le quote di Amazon nel. Riferimenti generali di Amazon Web Services

Autorizzazioni del ruolo collegato ai servizi per la protezione da malware

La protezione da malware utilizza il ruolo collegato ai servizi (SLR) denominato `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Questa reflex consente a Malware Protection di eseguire scansioni senza agenti per rilevare malware nel tuo account. GuardDuty Consente di GuardDuty creare un'istantanea del volume EBS nel tuo account e condividerla con l'account del servizio. GuardDuty Dopo aver GuardDuty valutato l'istantanea, include i metadati del carico di lavoro dell'istanza EC2 e del contenitore recuperati nei risultati di Malware Protection. Ai fini dell'assunzione del ruolo `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, il ruolo collegato ai servizi `malware-protection.guardduty.amazonaws.com`considera attendibile il servizio.

Le politiche di autorizzazione per questo ruolo aiutano Malware Protection a svolgere le seguenti attività:

- Usa le azioni di Amazon Elastic Compute Cloud (Amazon EC2) per recuperare informazioni sulle istanze, i volumi e le istantanee di Amazon EC2. La protezione da malware fornisce anche l'autorizzazione per accedere ai metadati dei cluster Amazon EKS e Amazon ECS.
- Crea snapshot per volumi EBS con il tag `GuardDutyExcluded` non impostato su `true`. Per impostazione predefinita, gli snapshot vengono creati con un tag `GuardDutyScanId`. Non rimuovere questo tag, altrimenti la protezione da malware non avrà accesso agli snapshot.

  > **Important**
  >
  > Se lo `GuardDutyExcluded` imposti su`true`, il GuardDuty servizio non sarà in grado di accedere a queste istantanee in futuro. Questo perché le altre istruzioni di questo ruolo collegato al servizio GuardDuty impediscono di eseguire qualsiasi azione sulle istantanee che hanno impostato su. `GuardDutyExcluded` `true`

- Consenti la condivisione e l'eliminazione degli snapshot solo se il tag `GuardDutyScanId` esiste e se il tag `GuardDutyExcluded` non è impostato su `true`.

> **Note**
>
> Ciò non consente alla protezione da malware di rendere pubblici gli snapshot.

- Accedi alle chiavi gestite dal cliente, ad eccezione di quelle con un `GuardDutyExcluded` tag impostato su`true`, da chiamare per creare e accedere `CreateGrant` a un volume EBS crittografato dall'istantanea crittografata che viene condivisa con l'account del servizio. GuardDuty Per un elenco degli account di GuardDuty servizio per ogni regione, consulta. GuardDuty account di servizio di Regione AWS
- Accedi ai CloudWatch log dei clienti per creare il gruppo di log Malware Protection e inserire i registri degli eventi di scansione antimalware nel `/aws/guardduty/malware-scan-events` gruppo di log.
- Consenti al cliente di decidere se conservare nel proprio account gli snapshot su cui è stato rilevato il malware. Se la scansione rileva malware, il ruolo collegato al servizio consente di aggiungere due tag GuardDuty alle istantanee: e. `GuardDutyFindingDetected` `GuardDutyExcluded`

> **Note**
>
> Il tag `GuardDutyFindingDetected` specifica che gli snapshot contengono malware.

- Determina se un volume è crittografato con una chiave gestita da EBS. GuardDuty esegue l'`DescribeKey`azione per determinare la `key Id` chiave gestita da EBS nel tuo account.
- Recupera l'istantanea dei volumi EBS crittografati utilizzando Chiave gestita da AWS, dal tuo Account AWS e copiala su. GuardDuty account di servizio A tal fine, utilizziamo le autorizzazioni e. `GetSnapshotBlock` `ListSnapshotBlocks` GuardDuty eseguirà quindi la scansione dell'istantanea nell'account del servizio. Attualmente, il supporto Malware Protection per la scansione dei volumi EBS crittografati con Chiave gestita da AWS potrebbe non essere disponibile in tutti i. Regioni AWS Per ulteriori informazioni, consulta Disponibilità di funzionalità specifiche per ogni regione.
- Consenti ad Amazon EC2 di effettuare chiamate per AWS KMS conto di Malware Protection per eseguire diverse azioni crittografiche sulle chiavi gestite dal cliente. Operazioni come `kms:ReEncryptTo` e `kms:ReEncryptFrom` sono necessarie per condividere gli snapshot crittografati con le chiavi gestite dal cliente. Sono accessibili solo le chiavi per le quali il tag `GuardDutyExcluded` non è impostato su `true`.

Il ruolo è configurato con le seguenti policy gestite da AWS, denominate `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "DescribeAndListPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ecs:ListClusters",
                "ecs:ListContainerInstances",
                "ecs:ListTasks",
                "ecs:DescribeTasks",
                "eks:DescribeCluster"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateSnapshotVolumeConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:volume/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "CreateSnapshotConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyScanId"
                }
            }
        },
        {
```

```
            "Sid": "CreateTagsPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:*/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSnapshot"
                }
            }
        },
        {
            "Sid": "AddTagsToSnapshotPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyExcluded",
                        "GuardDutyFindingDetected"
                    ]
                }
            }
        },
        {
            "Sid": "DeleteAndShareSnapshotPermission",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot",
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
```

```
        {
            "Sid": "PreventPublicAccessToSnapshotPermission",
            "Effect": "Deny",
            "Action": [
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:Add/group": "all"
                }
            }
        },
        {
            "Sid": "CreateGrantPermission",
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:ebs:id": "snap-*"
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Decrypt",
                        "CreateGrant",
                        "GenerateDataKeyWithoutPlaintext",
                        "ReEncryptFrom",
                        "ReEncryptTo",
                        "RetireGrant",
                        "DescribeKey"
                    ]
                },
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Sid": "ShareSnapshotKMSPermission",
            "Effect": "Allow",
```

```
            "Action": [
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "ec2.*.amazonaws.com"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "DescribeKeyPermission",
            "Effect": "Allow",
            "Action": "kms:DescribeKey",
            "Resource": "arn:aws:kms:*:*:key/*"
        },
        {
            "Sid": "GuardDutyLogGroupPermission",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:CreateLogGroup",
                "logs:PutRetentionPolicy"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
        },
        {
            "Sid": "GuardDutyLogStreamPermission",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
        },
        {
            "Sid": "EBSDirectAPIPermissions",
            "Effect": "Allow",
            "Action": [
```

```
                "ebs:GetSnapshotBlock",
                "ebs:ListSnapshotBlocks"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/GuardDutyScanId": "*"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        }
    ]
}
```

La policy di attendibilità seguente è associata al ruolo collegato ai servizi `AWSServiceRoleForAmazonGuardDutyMalwareProtection`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Creazione di un ruolo collegato ai servizi per la protezione da malware

Il ruolo collegato ai servizi `AWSServiceRoleForAmazonGuardDutyMalwareProtection` viene automaticamente creato quando abiliti la protezione da malware per la prima volta o quando la abiliti in una regione supportata in cui in precedenza era disabilitata. Puoi anche creare il ruolo collegato ai servizi `AWSServiceRoleForAmazonGuardDutyMalwareProtection` manualmente, utilizzando la console IAM, la CLI IAM o l'API IAM.

> **Note**
>
> Per impostazione predefinita, se sei un nuovo utente di Amazon GuardDuty, Malware Protection è abilitata automaticamente.

> **Important**
>
> Il ruolo collegato al servizio creato per l'account GuardDuty amministratore delegato non si applica agli account dei membri. GuardDuty

Per consentire a un principale IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. `AWSServiceRoleForAmazonGuardDutyMalwareProtection`Affinché il ruolo collegato al servizio venga creato correttamente, l'identità IAM con cui utilizzi deve disporre delle autorizzazioni GuardDuty richieste. Per concedere le autorizzazioni richieste, collega la seguente policy gestita a questo utente, gruppo o ruolo .

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

Per ulteriori informazioni sulla creazione manuale del ruolo, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente IAM.

Modifica di un ruolo collegato ai servizi per la protezione da malware

La protezione da malware non consente di modificare il ruolo collegato ai servizi `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per la protezione da malware

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non hai un'entità non utilizzata che non viene monitorata o gestita attivamente.

> **Important**
>
> Per eliminare il `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, devi prima disabilitare la protezione da malware in tutte le regioni in cui è abilitata.

Se la protezione da malware non è disabilitata quando tanti di eliminare il ruolo collegato ai servizi, l'eliminazione avrà esito negativo. Per ulteriori informazioni, consulta Per abilitare o disabilitare la scansione GuardDuty antimalware avviata.

Quando scegli Disabilita per interrompere il servizio di protezione da malware, il `AWSServiceRoleForAmazonGuardDutyMalwareProtection` non viene eliminato automaticamente. Se poi scegli Abilita per avviare nuovamente il servizio Malware Protection, GuardDuty inizierà a utilizzare quello esistente. `AWSServiceRoleForAmazonGuardDutyMalwareProtection`

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM, la AWS CLI o l'API IAM per eliminare il ruolo collegato al `AWSServiceRoleForAmazonGuardDutyMalwareProtection` servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Supportato Regioni AWS

Amazon GuardDuty supporta l'utilizzo del ruolo `AWSServiceRoleForAmazonGuardDutyMalwareProtection` collegato al servizio in tutti i casi in Regioni AWS cui è disponibile Malware Protection.

Per un elenco delle regioni in cui GuardDuty è attualmente disponibile, consulta gli GuardDuty endpoint e le quote di Amazon nel. Riferimenti generali di Amazon Web Services

> **Note**
>
> La protezione da malware non è attualmente disponibile negli AWS GovCloud Stati Uniti orientali e AWS GovCloud negli Stati Uniti occidentali.

Risoluzione dei problemi relativi all' GuardDuty identità e all'accesso ad Amazon

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con GuardDuty e IAM.

Argomenti

- Non sono autorizzato a eseguire alcuna azione in GuardDuty
- Non sono autorizzato a eseguire iam:PassRole.
- Voglio consentire a persone esterne Account AWS a me di accedere alle mie GuardDuty risorse.

Non sono autorizzato a eseguire alcuna azione in GuardDuty

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `guardduty:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 guardduty:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `guardduty:`*`GetWidget`*.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam:PassRole.

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a GuardDuty.

Alcuni Servizi AWS consentono di trasmettere un ruolo esistente a tale servizio, invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in GuardDuty. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne Account AWS a me di accedere alle mie GuardDuty risorse.

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se GuardDuty supporta queste funzionalità, consultaCome GuardDuty funziona Amazon con IAM.
- Per informazioni su come garantire l'accesso alle risorse negli Account AWS che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di proprietà dell'utente nella Guida per l'utente di IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWS di terze parti, consulta Fornire l'accesso agli Account AWS di proprietà di terze parti nella Guida per l'utente di IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

AWS politiche gestite per Amazon GuardDuty

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le politiche AWS gestite che scrivere le politiche da soli. Creare policy gestite dal cliente IAM per fornire al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste policy coprono i casi d'uso comuni e sono disponibili

nel tuo Account AWS. Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi aggiungono occasionalmente autorizzazioni aggiuntive a una policy AWS gestita per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una politica AWS gestita quando viene lanciata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy ReadOnlyAccess AWS gestita fornisce l'accesso in sola lettura a tutti i AWS servizi e le risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consulta la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

AWS politica gestita: AmazonGuardDutyFullAccess

È possibile allegare la policy `AmazonGuardDutyFullAccess`alle identità IAM.

Questa politica concede autorizzazioni amministrative che consentono a un utente l'accesso completo a tutte le GuardDuty azioni.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `GuardDuty`— Consente agli utenti l'accesso completo a tutte le GuardDuty azioni.
- `IAM`— Consente agli utenti di creare il ruolo GuardDuty collegato al servizio. Ciò consente a un GuardDuty amministratore di abilitare gli account GuardDuty dei membri.
- `Organizations`— Consente agli utenti di designare un amministratore delegato e gestire i membri di un' GuardDuty organizzazione.

L'autorizzazione a eseguire un'operazione `iam:GetRole` su `AWSServiceRoleForAmazonGuardDutyMalwareProtection` stabilisce se il ruolo collegato ai servizi (SLR) per la protezione da malware esiste in un account.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonGuardDutyFullAccessSid1",
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleSid1",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "guardduty.amazonaws.com",
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "ActionsForOrganizationsSid1",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IamGetRoleSid1",
            "Effect": "Allow",
            "Action": "iam:GetRole",
```

```
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

AWS politica gestita: AmazonGuardDutyReadOnlyAccess

È possibile allegare la policy `AmazonGuardDutyReadOnlyAccess`alle identità IAM.

Questa politica concede autorizzazioni di sola lettura che consentono a un utente di visualizzare GuardDuty i risultati e i dettagli dell'organizzazione. GuardDuty

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `GuardDuty`— Consente agli utenti di visualizzare GuardDuty i risultati ed eseguire operazioni API che iniziano con`Get`, o. `List` `Describe`
- `Organizations`— Consente agli utenti di recuperare informazioni sulla configurazione GuardDuty dell'organizzazione, inclusi i dettagli dell'account amministratore delegato.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:Describe*",
                "guardduty:Get*",
                "guardduty:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
```

```
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politica gestita: AmazonGuardDutyServiceRolePolicy

Non è possibile collegare `AmazonGuardDutyServiceRolePolicy`alle entità IAM. Questa policy AWS gestita è associata a un ruolo collegato al servizio che consente di eseguire azioni GuardDuty per conto dell'utente. Per ulteriori informazioni, consulta Autorizzazioni di ruolo collegate al servizio per GuardDuty.

GuardDuty aggiornamenti alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite GuardDuty da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei GuardDuty documenti.

Modifica	Descrizione	Data
AmazonGuardDutyServiceRolePolicy: aggiorna a una policy esistente.	Usa AWS Systems Manager le azioni per gestire le associazioni SSM sulle istanze Amazon EC2 quando GuardDuty abiliti il monitoraggio del runtime con agente automatizzato per Amazon EC2. Quando la configurazione GuardDuty automatizzata degli agenti è disabilitata, GuardDuty considera solo le istanze EC2 che hanno un tag di inclusione (:). `GuardDuty Managed true`	26 marzo 2024

Modifica	Descrizione	Data
AmazonGuardDutyServiceRolePolicy: aggiorna a una policy esistente.	GuardDuty ha aggiunto una nuova autorizzazione: `organization:DescribeOrganization` recuperare l'ID dell'organizzazione dell'account Amazon VPC condiviso e impostare la policy degli endpoint Amazon VPC con l'ID dell'organizzazione.	9 febbraio 2024
AmazonGuardDutyMalwareProtectionServiceRolePolitica: aggiornamento a una politica esistente.	Malware Protection ha aggiunto due autorizzazioni: `GetSnapshotBlock` quella di `ListSnapshotBlocks` recuperare l'istantanea di un volume EBS (con crittografia Chiave gestita da AWS) dall'utente Account AWS e copiarla sull'account del GuardDuty servizio prima di avviare la scansione antimalware.	25 gennaio 2024
AmazonGuardDutyServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte nuove autorizzazioni per consentire di GuardDuty aggiungere l'impostazione dell'account `guarddutyActivate` Amazon ECS ed eseguire operazioni, elencare e descrivere sui cluster Amazon ECS.	26 novembre 2023

Modifica	Descrizione	Data
AmazonGuardDutyReadOnlyAccess: aggiornamento a una policy esistente	GuardDuty ha aggiunto una nuova politica `organizations` per. `ListAccounts`	16 novembre 2023
AmazonGuardDutyFullAccess: aggiornamento a una policy esistente	GuardDuty ha aggiunto una nuova politica `organizations` per`ListAccounts` .	16 novembre 2023
AmazonGuardDutyServiceRolePolicy: aggiornamento a una policy esistente	GuardDuty ha aggiunto nuove autorizzazioni per supportare la prossima funzionalità GuardDuty EKS Runtime Monitoring.	8 marzo 2023

Modifica	Descrizione	Data
AmazonGuardDutyServiceRolePolicy: aggiornamento a una policy esistente	GuardDuty ha aggiunto nuove autorizzazioni per consentire la creazione di ruoli collegati GuardDuty al servizio per Malware Protection. Ciò contribuirà a GuardDuty semplificare il processo di attivazione della protezione da malware. GuardDuty ora può eseguire la seguente azione IAM: `{ "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com" } } }`	21 febbraio 2023
AmazonGuardDutyFullAccess: aggiornamento a una policy esistente	GuardDuty ARN aggiornato per `iam:GetRole` to. `*AWSServiceRoleForAmazonGuardDutyMalwareProtection`	26 luglio 2022

Modifica	Descrizione	Data
AmazonGuardDutyFullAccess: aggiornamento a una policy esistente	GuardDuty ha aggiunto un nuovo `AWSServiceName` per consentire la creazione di ruoli collegati al servizio utilizzando il servizio GuardDuty Malware `iam:CreateServiceLinkedRole` Protection. GuardDuty ora può eseguire l'`iam:GetRole` azione per ottenere informazioni per. `AWSServiceRole`	26 luglio 2022

Modifica	Descrizione	Data
AmazonGuardDutyServiceRolePolicy: aggiornamento a una policy esistente	GuardDuty ha aggiunto nuove autorizzazioni per consentire di GuardDuty utilizzare le azioni di rete di Amazon EC2 per migliorare i risultati. GuardDuty ora puoi eseguire le seguenti azioni EC2 per ottenere informazioni su come comunicano le tue istanze EC2. Queste informazioni vengono utilizzate per migliorare la precisione degli esiti. • `ec2:DescribeVpcEndpoints` • `ec2:DescribeSubnets` • `ec2:DescribeVpcPeeringConnections` • `ec2:DescribeTransitGatewayAttachments`	3 agosto 2021
GuardDuty ha iniziato a tenere traccia delle modifiche	GuardDuty ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	3 agosto 2021

Convalida della conformità per Amazon GuardDuty

Per sapere se il Servizio AWS è coperto da programmi di conformità specifici, consulta i Servizi AWS coperti dal programma di conformità e scegli il programma di conformità desiderato. Per informazioni generali, consulta Programmi per la conformità di AWS.

È possibile scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Download di report in AWS Artifact.

La responsabilità di conformità durante l'utilizzo dei Servizi AWS è determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle normative vigenti. Per semplificare il rispetto della conformità, AWS mette a disposizione le seguenti risorse:

- Guide Quick Start per la sicurezza e conformità: queste guide all'implementazione illustrano considerazioni relative all'architettura e forniscono la procedura per l'implementazione di ambienti di base su AWS incentrati sulla sicurezza e sulla conformità.
- Architetture per la sicurezza e la conformità HIPAA su Amazon Web Services: questo whitepaper descrive come le aziende possono utilizzare AWS per creare applicazioni conformi alla normativa HIPAA.

  > **Note**
  >
  > Non tutti i Servizi AWS sono conformi ai requisiti HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- Risorse per la conformità AWS: una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- Guide alla conformità per i clienti AWS: acquisisci nozioni sul modello di responsabilità condivisa attraverso la lente di conformità. Le guide riassumono le best practice per la protezione dei Servizi AWS e tracciano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con le regole nella Guida per gli sviluppatori di AWS Config: il servizio AWS Config valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti.
- AWS Security Hub: questo Servizio AWS fornisce una visione completa dello stato di sicurezza all'interno di AWS. La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- AWS Audit Manager: questo Servizio AWS aiuta a effettuare un audit costante dell'utilizzo di AWS per semplificare la gestione dei rischi e della conformità alle normative e agli standard di settore.

Resilienza in Amazon GuardDuty

L'infrastruttura globale di AWS è basata su regioni AWS e zone di disponibilità. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le Zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili, rispetto alle infrastrutture a data center singolo o multiplo.

Per ulteriori informazioni sulle Regioni e le Zone di disponibilità AWS, consulta Infrastruttura globale di AWS.

Sicurezza dell'infrastruttura in Amazon GuardDuty

In qualità di servizio gestito, Amazon GuardDuty è protetto dalla sicurezza di rete globale di AWS. Per informazioni sui servizi di sicurezza AWS e su come AWS protegge l'infrastruttura, consulta la pagina Sicurezza del cloud AWS. Per progettare l'ambiente AWS utilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina Protezione dell'infrastruttura nel Pilastro della sicurezza di AWS Well-Architected Framework.

Utilizza le chiamate API pubblicate da AWS per accedere a GuardDuty tramite la rete. I clienti devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Integrazioni di servizi AWS con GuardDuty

GuardDuty può essere integrato con altri servizi di sicurezza AWS. Questi servizi possono importare dati da GuardDuty per consentirti di visualizzare gli esiti in modi nuovi. Consulta le seguenti opzioni di integrazione per saperne di più sul modo in cui i servizi sono configurati per funzionare con GuardDuty.

Integrazione di GuardDuty con AWS Security Hub

AWS Security Hub raccoglie i dati di sicurezza da diversi account e servizi AWS e prodotti supportati di partner di terze parti per valutare lo stato di sicurezza del tuo ambiente in base agli standard e alle best practice di settore. Oltre a valutare il tuo livello di sicurezza, Security Hub crea una posizione centrale per gli esiti di tutti i servizi integrati AWS e i prodotti dei partner AWS. L'abilitazione di Security Hub con GuardDuty consentirà automaticamente l'acquisizione dei dati degli esiti di GuardDuty da parte di Security Hub.

Per ulteriori informazioni sull'utilizzo di Security Hub con GuardDuty, consulta Integrazione con AWS Security Hub.

Integrazione di GuardDuty con Amazon Detective

Amazon Detective utilizza i dati di log provenienti da tutti i tuoi account AWS per creare visualizzazioni di dati per le tue risorse e gli indirizzi IP che interagiscono con il tuo ambiente. Le visualizzazioni di Detective sono utili per indagare in modo rapido e semplice sui problemi di sicurezza. Una volta abilitati entrambi i servizi, puoi passare dai dettagli degli esiti di GuardDuty alle informazioni nella console Detective.

Per ulteriori informazioni sull'utilizzo di Detective con GuardDuty, consulta Integrazione con Amazon Detective.

Integrazione con AWS Security Hub

AWS Security Hub fornisce una visione completa dello stato di sicurezza in AWS e ti aiuta a controllare l'ambiente rispetto agli standard di sicurezza del settore e alle best practice. Security Hub raccoglie dati sulla sicurezza da tutti AWS gli account, i servizi e i prodotti partner di terze parti

supportati e ti aiuta ad analizzare le tendenze in materia di sicurezza e identificare i problemi di sicurezza con la massima priorità.

L' GuardDuty integrazione di Amazon con Security Hub ti consente di inviare i risultati GuardDuty da Security Hub. Security Hub può quindi includere tali risultati nella sua analisi della posizione di sicurezza.

Indice

- In che modo Amazon GuardDuty invia i risultati a AWS Security Hub
  - Tipi di risultati che vengono GuardDuty inviati a Security Hub
    - Latenza per l'invio di nuovi risultati
    - Nuovo tentativo quando Security Hub non è disponibile
    - Aggiornamento degli esiti esistenti nella Centrale di sicurezza
- Visualizzazione dei risultati GuardDuty in AWS Security Hub
  - Interpretazione dei nomi GuardDuty dei risultati in AWS Security Hub
  - Esito tipico di GuardDuty
- Abilitazione e configurazione dell'integrazione
- Interruzione dell'invio degli esiti a Security Hub

In che modo Amazon GuardDuty invia i risultati a AWS Security Hub

Nel AWS Security Hub, i problemi di sicurezza vengono registrati come risultati. Alcuni risultati derivano da problemi rilevati da altri AWS servizi o da partner terzi. Security Hub dispone inoltre di una serie di regole che utilizza per rilevare problemi di sicurezza e generare risultati.

Security Hub fornisce strumenti per gestire i risultati da tutte queste fonti. È possibile visualizzare e filtrare gli elenchi di risultati e visualizzare i dettagli per un riscontro. Per ulteriori informazioni, consulta Visualizzazione dei riscontri nella Guida per l'utente AWS Security Hub . È inoltre possibile monitorare lo stato di un'indagine in un esito. Per ulteriori informazioni, consulta Azioni sugli esiti nella Guida per l'utente di AWS Security Hub .

Tutti i risultati in Security Hub utilizzano un formato JSON standard chiamato AWS Security Finding Format (ASFF). L'ASFF include dettagli sull'origine del problema, sulle risorse interessate e sullo stato corrente del risultato. Consulta AWS Security Finding Format (ASFF) nella Guida per l'utente di AWS Security Hub .

Amazon GuardDuty è uno dei AWS servizi che invia i risultati a Security Hub.

Tipi di risultati che vengono GuardDuty inviati a Security Hub

Una volta abilitato GuardDuty Security Hub nello stesso account all'interno dello stesso Regione AWS, GuardDuty inizia a inviare tutti i risultati generati a Security Hub. Questi risultati vengono inviati a Security Hub utilizzando il AWS Security Finding Format (ASFF). In ASFF, il `Types` campo fornisce il tipo di esito.

Latenza per l'invio di nuovi risultati

Quando viene GuardDuty creato un nuovo risultato, di solito viene inviato a Security Hub entro cinque minuti.

Nuovo tentativo quando Security Hub non è disponibile

Se Security Hub non è disponibile, GuardDuty riprova a inviare i risultati finché non vengono ricevuti.

Aggiornamento degli esiti esistenti nella Centrale di sicurezza

Dopo aver inviato un risultato a Security Hub, GuardDuty invia aggiornamenti per riflettere ulteriori osservazioni sull'attività di ricerca a Security Hub. Le nuove osservazioni di questi risultati vengono inviate a Security Hub in base alle Fase 5 — Frequenza di aggiornamento dell'esportazione impostazioni del tuo Account AWS.

Quando archivi o annulli l'archiviazione di un risultato, GuardDuty non lo invia a Security Hub. Qualsiasi risultato non archiviato manualmente e che successivamente diventerà attivo in non GuardDuty viene inviato a Security Hub.

Visualizzazione dei risultati GuardDuty in AWS Security Hub

Per visualizzare i GuardDuty risultati in Security Hub, seleziona See Findings under Amazon GuardDuty dalla pagina di riepilogo. In alternativa, puoi selezionare Risultati dal pannello di navigazione e filtrare i risultati per visualizzare solo GuardDuty i risultati selezionando il campo Nome prodotto: con un valore di`GuardDuty`.

Interpretazione dei nomi GuardDuty dei risultati in AWS Security Hub

GuardDuty invia i risultati a Security Hub utilizzando il AWS Security Finding Format (ASFF). In ASFF, il `Types` campo fornisce il tipo di esito. I tipi ASFF utilizzano uno schema di denominazione

diverso rispetto ai tipi. GuardDuty La tabella seguente descrive in dettaglio tutti i tipi GuardDuty di risultati con la loro controparte ASFF così come appaiono in Security Hub.

> **Note**
>
> Per alcuni tipi di GuardDuty ricerca, Security Hub assegna nomi di ricerca ASFF diversi a seconda che il ruolo della risorsa del dettaglio del risultato sia ACTOR o TARGET. Per ulteriori informazioni, consulta Dettagli degli esiti.

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulBruteForce
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulLogin
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.FailedLogin
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.SuccessfulLogin
CredentialAccess:RDS/TorIPCaller.FailedLogin	TTPs/Credential Access/RDS-TorIPCaller.FailedLogin
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-TorIPCaller.SuccessfulLogin

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B
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
DefenseEvasiontipo di ricerca ----sep----:IAMUser/ AnomalousBehavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/PtraceAntiDebugging	TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging
DefenseEvasion:Runtime/SuspiciousCommand	TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand

GuardDuty tipo di ricerca	Tipo di risultati ASFF
Scoperta: iamUser/ AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
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
Execution:Kubernetes/AnomalousBehavior.ExecInPod	TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer
Execution:EC2/MaliciousFile	TTPs/Execution/Execution:EC2-MaliciousFile
Execution:ECS/MaliciousFile	TTPs/Execution/Execution:ECS-MaliciousFile

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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:Runtime/MaliciousFileExecuted	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted
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/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
Impact:EC2/SuspiciousDomainRequest.Reputation	TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation
Impact:EC2/WinRMBruteForce	TTPs/Impact/Impact:EC2-WinRMBruteForce
Impatto: iamUser/ AnomalousBehavior	TTPs/Impact/IAMUser-AnomalousBehavior
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
InitialAccessImpatto: iamUser/ ----sep----:iamUser/ AnomalousBehavior	TTPs/Initial Access/IAMUser-AnomalousBehavior
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
Persistenza: 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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
Policy:IAMUser/RootCredentialUsage	TTPs/Policy:IAMUser-RootCredentialUsage
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
PrivilegeEscalationPersistenza: iamUser/ ----sep----:iamUser/ AnomalousBehavior	TTPs/Privilege Escalation/IAMUser-AnomalousBehavior
PrivilegeEscalation:IAMUser/AdministrativePermissions	TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	TTPs/AnomalousBehavior/PriviledgeEscalation:Kubernetes-RoleBindingCreated
PriviledgeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	TTPs/AnomalousBehavior/PriviledgeEscalation:Kubernetes-RoleCreated
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/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
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
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

GuardDuty tipo di ricerca	Tipo di risultati ASFF
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/Unauthorized Access:IAMUser-ConsoleLogin
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS
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/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 tipo di ricerca	Tipo di risultati 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

Esito tipico di GuardDuty

GuardDuty invia i risultati a Security Hub utilizzando il AWS Security Finding Format (ASFF).

Ecco un esempio di un risultato tipico di 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"
}
```


Abilitazione e configurazione dell'integrazione

Per utilizzare l'integrazione con AWS Security Hub, è necessario abilitare Security Hub. Per informazioni su come abilitare Security Hub, consulta Configurazione di Security Hub nella Guida per l'utente di AWS Security Hub .

Quando abiliti entrambi GuardDuty e Security Hub, l'integrazione viene abilitata automaticamente. GuardDutyinizia immediatamente a inviare i risultati a Security Hub.

Interruzione dell'invio degli esiti a Security Hub

Per interrompere l'invio dei risultati a Security Hub, puoi utilizzare la console o l'API di Security Hub.

Vedi Disabilitazione e abilitazione del flusso di risultati da un'integrazione (console) o Disabilitazione del flusso di risultati da un'integrazione (Security Hub API, AWS CLI) nella Guida per l'utente.AWS Security Hub

Integrazione con Amazon Detective

Amazon Detective è utile per analizzare e indagare rapidamente sugli eventi di sicurezza su uno o più account AWS tramite la generazione di visualizzazioni di dati che rappresentano il modo in cui le tue risorse si comportano e interagiscono nel tempo. Detective crea visualizzazioni degli esiti di GuardDuty.

Detective acquisisce i dettagli di tutti ogni tipo di esito e fornisce l'accesso ai profili delle entità per indagare su quelle coinvolte negli esiti. Un'entità può essere un Account AWS, una risorsa AWS all'interno di un account o un indirizzo IP esterno che ha interagito con le tue risorse. La console GuardDuty supporta il passaggio ad Amazon Detective dalle seguenti entità, a seconda del tipo di esito: Account AWS, ruolo, utente o sessione di ruolo IAM, agente utente, utente federato, istanza Amazon EC2 o indirizzo IP.

Indice

- Abilitazione dell'integrazione
- Passaggio ad Amazon Detective da un esito di GuardDuty
- Utilizzo dell'integrazione con un ambiente multi-account GuardDuty

Abilitazione dell'integrazione

Devi abilitare Amazon Detective prima di poterlo utilizzare con GuardDuty. Per informazioni su come abilitare Detective, consulta Configurazione di Amazon Detective nella Guida di amministrazione di Amazon Detective.

Quando abiliti GuardDuty e Detective, l'integrazione viene abilitata automaticamente. Dopo l'abilitazione, Detective acquisirà immediatamente i dati degli esiti di GuardDuty.

> **Note**
>
> GuardDuty invia gli esiti a Detective in base alla frequenza di esportazione degli esiti di GuardDuty. Per impostazione predefinita, la frequenza di esportazione per gli aggiornamenti agli esiti esistenti è di 6 ore. Per garantire che Detective riceva gli aggiornamenti più recenti sugli esiti, ti consigliamo di modificare la frequenza di esportazione affinché avvenga ogni 15 minuti in tutte le regioni in cui usi Detective con GuardDuty. Per ulteriori informazioni, consulta Passaggio 5: impostazione della frequenza per esportare i risultati attivi aggiornati.

Passaggio ad Amazon Detective da un esito di GuardDuty

1. Accedi alla console https://console.aws.amazon.com/guardduty/.
2. Scegli un singolo esito dalla tabella degli esiti.
3. Scegli Esamina con Detective dal riquadro dei dettagli dell'esito.
4. Scegli un aspetto dell'esito su cui indagare con Amazon Detective. Così facendo si apre la console Detective per l'esito o entità in questione.

Se il pivot non si comporta come previsto, consulta Risoluzione dei problemi del pivot nella nella Guida per l'utente di Amazon Detective.

> **Note**
>
> Se archivi un esito di GuardDuty nella console Detective, lo stesso esito viene archiviato anche nella console GuardDuty.

Utilizzo dell'integrazione con un ambiente multi-account GuardDuty

Se gestisci un ambiente multi-account in GuardDuty, devi aggiungere i tuoi account membri ad Amazon Detective per accedere alle visualizzazioni dei dati di Detective relativi agli esiti e alle entità presenti in tali account.

Ti consigliamo di utilizzare lo stesso account amministratore GuardDuty dell'account amministratore impiegato per Detective. Per ulteriori informazioni sull'aggiunta di account membri in Detective, consulta Invitare account membri.

> **Note**
>
> Detective è un servizio regionale, perciò devi abilitare Detective e aggiungere i tuoi account membri in ogni regione in cui desideri utilizzare l'integrazione.

Sospensione o disabilitazione GuardDuty

Puoi utilizzare la GuardDuty console per sospendere o disabilitare il servizio. GuardDuty Non ti viene addebitato alcun costo per l'utilizzo GuardDuty quando il servizio è sospeso.

- Tutti gli account dei membri devono essere dissociati o eliminati prima di poter sospendere o disabilitare. GuardDuty
- Se si sospende GuardDuty, la sospensione non monitora più la sicurezza dell' AWS ambiente né genera nuovi risultati. I risultati esistenti rimangono intatti e non sono influenzati dalla sospensione. GuardDuty Puoi scegliere di GuardDuty riattivarla in un secondo momento.
- La disattivazione GuardDuty in un account verrà disattivata solo per l'account attualmente selezionato Regione AWS. Se desideri disabilitarlo completamente GuardDuty, devi disabilitarlo in ogni regione in cui è abilitato.
- Se disabiliti GuardDuty, i risultati e la GuardDuty configurazione esistenti vengono persi e non possono essere recuperati. Se desideri salvare i risultati esistenti, devi esportarli prima di confermarne la disabilitazione GuardDuty. Per informazioni su come esportare gli esiti, consulta Esportazione degli esiti.

Per sospendere o disabilitare GuardDuty

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella GuardDuty sezione Sospendi, scegli Sospendi GuardDuty o Disattiva GuardDuty, quindi Conferma l'azione.

Da riattivare dopo la sospensione GuardDuty

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione scegli Impostazioni.
3. Scegli Riattiva. GuardDuty

Iscrizione agli annunci di Amazon SNS GuardDuty

Questa sezione fornisce informazioni sulla sottoscrizione ad Amazon SNS (Simple Notification Service) GuardDuty per gli annunci di ricezione di notifiche sui tipi di risultati appena rilasciati, aggiornamenti ai tipi di risultati esistenti e altre modifiche alle funzionalità. Le notifiche sono disponibili in tutti i formati supportati da Amazon SNS.

Il GuardDuty SNS invia annunci sugli aggiornamenti del GuardDuty servizio a qualsiasi account sottoscritto. AWS Per ricevere notifiche sugli esiti all'interno del tuo account, consulta Creazione di risposte personalizzate ai GuardDuty risultati con Amazon CloudWatch Events.

> **Note**
>
> Il tuo utente IAM deve disporre delle autorizzazioni `sns::subscribe` per sottoscrivere un argomento SNS.

Puoi sottoscrivere una coda Amazon SQS a questo argomento di notifica, ma devi utilizzare un ARN dell'argomento che si trovi nella stessa regione. Per ulteriori informazioni, consulta Tutorial: sottoscrizione di una coda Amazon SQS a un argomento Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Queue Service.

Puoi anche utilizzare una AWS Lambda funzione per attivare eventi quando vengono ricevute notifiche. Per ulteriori informazioni, consulta Richiamo delle funzioni Lambda tramite le notifiche di Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Queue Service.

Di seguito vengono mostrati gli ARN dell'argomento Amazon SNS per ogni regione.

AWS Regione	ARN di un argomento Amazon SNS
`us-east-1`	`arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements`
`us-east-2`	`arn:aws:sns:us-east-2:118283430703:G`

AWS Regione	ARN di un argomento Amazon SNS
	uardDutyAnnouncements
us-west-1	arn:aws:sns:us-west-1:144182107116:GuardDutyAnnouncements
us-west-2	arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements
ca-central-1	arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnouncements
ca-west-1	arn:aws:sns:ca-west-1:440427180217:GuardDutyAnnouncements
eu-north-1	arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnouncements
eu-west-1	arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnouncements

AWS Regione	ARN di un argomento Amazon SNS
eu-west-2	arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements
eu-west-3	arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements
eu-central-1	arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements
eu-central-2	arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements
ap-east-1	arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements
ap-northeast-1	arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements
ap-northeast-2	arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements

AWS Regione	ARN di un argomento Amazon SNS
ap-southeast-1	arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements
ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements
ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements
sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements
us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements
cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements
cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements

AWS Regione	ARN di un argomento Amazon SNS
me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements
me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements
eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements

AWS Regione	ARN di un argomento Amazon SNS
ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements
ap-southeast-4	arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements
il-central-1	arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements

Per iscriverti all'e-mail di notifica dell' GuardDuty aggiornamento nella AWS Management Console

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nell'elenco delle regioni, scegli la stessa regione dell'argomento ARN da sottoscrivere. Questo esempio utilizza la regione `us-west-2`.
3. Nel riquadro di navigazione a sinistra, scegli Subscriptions (Abbonamenti), quindi Create subscription (Crea abbonamento).
4. Nella finestra di dialogo Create Subscription (Crea sottoscrizione), in Topic ARN (ARN argomento), incolla l'ARN dell'argomento: `arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements`.
5. Per Protocollo, scegli E-mail. Per Endpoint, digitare l'indirizzo e-mail a cui deve essere inviata la notifica.
6. Scegli Crea sottoscrizione.
7. Nella tua applicazione di posta elettronica, apri il messaggio contenuto in AWS Notifiche e apri il link per confermare l'iscrizione.

   Nel Web browser viene visualizzata una risposta di conferma di Amazon SNS.

Per iscriverti all'e-mail di notifica dell' GuardDuty aggiornamento con AWS CLI

1. Esegui il comando riportato qui di seguito con la 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. Nella tua applicazione di posta elettronica, apri il messaggio contenuto in AWS Notifiche e apri il link per confermare l'iscrizione.

   Nel Web browser viene visualizzata una risposta di conferma di Amazon SNS.

Formato dei messaggi Amazon SNS

Di seguito è riportato un esempio di messaggio di notifica di GuardDuty aggiornamento relativo a nuovi risultati:

```
{
    "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"
}
```

Il valore Message analizzato (con la rimozione dei caratteri escape) viene mostrato di seguito:

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

Di seguito è riportato un esempio di messaggio di notifica di GuardDuty aggiornamento relativo agli aggiornamenti delle GuardDuty funzionalità:

```
{
    "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_cloudtrail\"}]}",
    "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"
}
```

Il valore Message analizzato (con la rimozione dei caratteri escape) viene mostrato di seguito:

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

Di seguito è riportato un esempio GuardDuty di messaggio di notifica di aggiornamento relativo ai risultati aggiornati:

```
{
    "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"
}
```

Il valore Message analizzato (con la rimozione dei caratteri escape) viene mostrato di seguito:

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

Quote per Amazon GuardDuty

L'account AWS dispone delle seguenti quote predefinite, precedentemente definite limiti, per ogni servizio AWS. Salvo dove diversamente specificato, ogni quota si applica a una regione specifica. Se per alcune quote è possibile richiedere aumenti, altre quote non possono essere modificate.

Per visualizzare le quote per GuardDuty, apri la console Service Quotas. Nel riquadro di navigazione, scegli AWSservizi e seleziona Amazon GuardDuty.

Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida dell'utente di Service Quotas.

Il tuo AWS account ha le seguenti quote per Amazon GuardDuty per regione.

> **Note**
>
> Per le quote specifiche per la protezione da GuardDuty malware, consulta. Quote di protezione da malware

Risorsa	Default	Commenti
Rilevatori	1	Il numero massimo di risorse del rilevatore che puoi creare per account AWS per regione. Non è possibile richiedere un aumento della quota.
Filtri	100	Il numero massimo di filtri salvati per account AWS per regione.

Risorsa	Default	Commenti
		Non è possibile richiedere un aumento della quota.
Ritrovamento del periodo di conservazione	90 giorni	Il numero massimo di giorni di accertamento viene mantenuto. Non è possibile richiedere un aumento della quota.
Indirizzi IP e intervalli CIDR per l'elenco degli IP affidabili	2.000	Il numero massimo di indirizzi IP e intervalli CIDR che è possibile includere in un singolo elenco di IP affidabili. Non è possibile richiedere un aumento della quota.
Indirizzi IP e intervalli CIDR per l'elenco delle minacce	250.000	Il numero massimo di indirizzi IP e intervalli CIDR che è possibile includere in un elenco di minacce. Non è possibile richiedere un aumento della quota.

Risorsa	Default	Commenti
Dimensione massima dei file	35 MB	La dimensione massima del file utilizzato per caricare un elenco di indirizzi IP o intervalli CIDR da includere in un elenco di IP affidabili o in un elenco di minacce. Non è possibile richiedere un aumento della quota.
Account membri (su invito)	5000	Il numero massimo di account membro associati a un account amministratore.
Account membri	50.000	Il numero massimo di account membro associati a un account amministratore tramiteAWS Organizations. inclusi gli account membri che vengono aggiunti all'organizzazione tramite invito.

Risorsa	Default	Commenti
Set di intelligence delle minacce	6	Il numero massimo di set di intelligence delle minacce che puoi aggiungere per account AWS per regione. Non è possibile richiedere un aumento della quota.
Set di IP affidabili	1	Numero massimo di set di IP affidabili che è possibile caricare e attivare per account AWS per regione. Non è possibile richiedere un aumento della quota.

Risoluzione dei problemi con Amazon GuardDuty

Se riscontri problemi relativi all'esecuzione di un'azione specifica di GuardDuty, consulta gli argomenti di questa sezione.

Argomenti

- Problemi generali in GuardDuty
- Problemi di protezione da malware
- Problemi di monitoraggio del runtime
- Gestione dei problemi relativi a più account
- Altre questioni relative alla risoluzione dei problemi

Problemi generali in GuardDuty

Ricevo un errore di accesso durante l'esportazione dei GuardDuty risultati. Come posso risolvere questo problema?

Dopo aver configurato le impostazioni per esportare i risultati, se non GuardDuty è possibile esportare i risultati, viene visualizzato un messaggio di errore nella pagina Impostazioni della GuardDuty console. Ciò può accadere potenzialmente quando non è più GuardDuty possibile accedere alla risorsa di destinazione, ad esempio se il bucket Amazon S3 è stato eliminato o l'autorizzazione per accedere al bucket è stata modificata. Ciò può verificarsi anche quando non è più GuardDuty possibile accedere alla AWS KMS chiave utilizzata per crittografare i dati nel bucket Amazon S3. Quando non GuardDuty è in grado di esportare, invia una notifica all'indirizzo e-mail associato all'account per fornire informazioni su questo problema.

Per risolvere il problema, assicurati che le risorse corrispondenti esistano e GuardDuty disponga delle autorizzazioni per accedere alle risorse necessarie. Se non risolvi il problema prima del termine del periodo di conservazione dei risultati di 90 giorni GuardDuty, i risultati non verranno esportati. GuardDuty disabiliterà la ricerca delle impostazioni di esportazione per questo account nella regione specifica. Anche dopo questa data di conservazione, è possibile aggiornare le impostazioni di configurazione per riavviare l'esportazione dei risultati nella regione specifica.

Per ulteriori informazioni, consulta Esportazione degli esiti.

Problemi di protezione da malware

All'avvio di una scansione antimalware on demand ricevo un messaggio di un errore che segnala la mancanza delle autorizzazioni richieste.

Se ricevi un errore che suggerisce che non disponi delle autorizzazioni necessarie per avviare una scansione antimalware on demand su un'istanza Amazon EC2, verifica di aver collegato la policy AWS politica gestita: AmazonGuardDutyFullAccess al tuo ruolo IAM.

Se sei membro di un' AWS organizzazione e continui a ricevere lo stesso errore, connettiti al tuo account di gestione. Per ulteriori informazioni, consulta AWS Organizations SCP — Accesso negato.

Ricevo un errore **`iam:GetRole`** mentre utilizzo la protezione da malware.

Se ricevi questo erroreUnable to get role: AWSServiceRoleForAmazonGuardDutyMalwareProtection, significa che non hai l'autorizzazione per abilitare la scansione antimalware GuardDuty avviata o utilizzare la scansione antimalware su richiesta. Verifica di aver collegato la policy AWS politica gestita: AmazonGuardDutyFullAccess al tuo ruolo IAM.

Sono un account GuardDuty amministratore che deve abilitare la scansione antimalware GuardDuty avviata dall'utente, ma non utilizza AWS Managed Policy: to manage. AmazonGuardDutyFullAccess GuardDuty

- Configura il ruolo IAM con cui utilizzi GuardDuty per disporre delle autorizzazioni necessarie per abilitare la scansione GuardDuty antimalware avviata. Per ulteriori informazioni sulle autorizzazioni necessarie, consulta Creazione di un ruolo collegato ai servizi per la protezione da malware.
- Collega AWS politica gestita: AmazonGuardDutyFullAccess al tuo ruolo IAM. Questo ti aiuterà ad abilitare la scansione antimalware GuardDuty avviata dall'utente per gli account dei membri.

Problemi di monitoraggio del runtime

Il mio AWS Step Functions flusso di lavoro non funziona in modo imprevisto

Se il GuardDuty contenitore ha contribuito all'errore del flusso di lavoro, vedi. Risoluzione dei problemi di copertura Se il problema persiste, per evitare che il flusso di lavoro non funzioni a causa del GuardDuty contenitore, esegui una delle seguenti operazioni:

- Aggiungi il `false` tag`GuardDutyManaged`: al cluster Amazon ECS associato.
- Disattiva la configurazione automatica degli agenti per AWS Fargate (solo ECS) a livello di account. Aggiungi il tag di inclusione`GuardDutyManaged`: `true` al cluster Amazon ECS associato che desideri continuare a monitorare con l'agente GuardDuty automatizzato.

Risoluzione degli errori di esaurimento della memoria in Runtime Monitoring (solo supporto Amazon EC2)

Questa sezione fornisce le procedure per la risoluzione dei problemi in caso di esaurimento della memoria in base Limite di CPU e memoria alla distribuzione manuale del GuardDuty Security Agent.

Se `systemd` interrompe l' GuardDuty agente a causa del `out-of-memory` problema e si ritiene che fornire più memoria all' GuardDuty agente sia ragionevole, è possibile aggiornare il limite.

1. Con l'autorizzazione root, apri`/lib/systemd/system/amazon-guardduty-agent.service`.
2. Trova `MemoryLimit` e `MemoryMax` aggiorna entrambi i valori.

```
MemoryLimit=256MB
MemoryMax=256MB
```

3. Dopo aver aggiornato i valori, riavviate l' GuardDuty agente utilizzando il seguente comando:

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. Eseguite il comando seguente per visualizzare lo stato:

```
sudo systemctl status amazon-guardduty-agent
```

   L'output previsto mostrerà il nuovo limite di memoria:

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

Gestione dei problemi relativi a più account

Desidero gestire più account ma non dispongo dell'autorizzazione di AWS Organizations gestione richiesta.

Se ricevi questo erroreThe `request failed because you do not have required AWS Organization master permission.`, significa che non hai l'autorizzazione per abilitare la scansione antimalware GuardDuty avviata per più account della tua organizzazione. Per ulteriori informazioni su come concedere l'autorizzazione all'account di gestione, consulta. Stabilire un accesso affidabile per abilitare la scansione GuardDuty antimalware avviata

Altre questioni relative alla risoluzione dei problemi

Se non trovi lo scenario adatto al tuo problema, visualizza le seguenti opzioni di risoluzione dei problemi:

- Per problemi generali relativi a IAM quando accedi a https://console.aws.amazon.com/guardduty/, consulta Risoluzione dei problemi relativi all' GuardDuty identità e all'accesso ad Amazon.
- Per problemi di autenticazione e autorizzazione durante l'accesso AWS AWS Console Home, consulta Risoluzione dei problemi di IAM.

Regioni ed endpoint

Per visualizzare Regioni AWS dove GuardDuty è disponibile Amazon, consulta Amazon GuardDuty endpoints nel Riferimenti generali di Amazon Web Services.

Ti consigliamo di abilitare tutte le GuardDuty funzionalità supportate Regioni AWS. Ciò consente di GuardDuty generare informazioni su attività non autorizzate o insolite anche nelle Regioni che non utilizzi attivamente. Ciò consente inoltre di GuardDuty monitorare AWS CloudTrail gli eventi per il soggetto supportato Regioni AWS, riducendo la sua capacità di rilevare attività che coinvolgono servizi globali.

Disponibilità di funzionalità specifiche per ogni regione

Un elenco di differenze regionali per specificare la disponibilità delle GuardDuty funzionalità.

ListFindings e GetFindingsStatistics API

Le ListFindingsAPI GetFindingsStatisticsand hanno un flag temporaneo`consoleOnly`. Quando utilizzi una o entrambe queste API, il `consoleOnly` flag indica che l'API può recuperare risultati fino a un limite massimo di 1000.

GuardDuty funzionalità con disparità di regione

GuardDuty Protezione da malware

GuardDuty supporta la funzionalità Malware Protection nelle AWS Dedicated Local Zones.

GuardDuty Monitoraggio del runtime

La funzionalità Runtime Monitoring non è attualmente supportata nella regione Canada occidentale (Calgary).

GuardDuty Protezione RDS

L'elenco seguente specifica i Regioni AWS casi in cui la protezione RDS non è attualmente supportata:

- Canada occidentale (Calgary)
- Asia Pacific (Hyderabad)
- Europa (Spagna)
- Europa (Zurigo)

- Medio Oriente (Emirati Arabi Uniti)
- Israele (Tel Aviv)
- Asia Pacifico (Melbourne)

Le seguenti API in Amazon GuardDuty API Reference possono presentare differenze regionali a causa dell'indisponibilità di alcune fonti di dati o funzionalità specificate in precedenza: Regioni AWS

- CreateDetector
- UpdateDetector
- UpdateMemberDetectors
- UpdateOrganizationConfiguration
- GetDetector
- GetMemberDetectors
- DescribeOrganizationConfiguration

Tipi di esiti di Amazon EC2: DefenseEvasion:EC2/UnusualDoHActivity e DefenseEvasion:EC2/UnusualDoTActivity

La tabella seguente mostra Regioni AWS dove GuardDuty è disponibile, ma questi due tipi di ricerca di Amazon EC2 non sono ancora supportati.

Regione AWS	Codice regione
Asia Pacifico (Seoul)	ap-northeast-2
Asia Pacifico (Osaka-Locale)	ap-northeast-3
Asia Pacifico (Giacarta)	ap-southeast-3

AWS GovCloud (US) Regioni

Per le informazioni più recenti, consulta Amazon GuardDuty nella Guida AWS GovCloud (US) per l'utente.

Regioni della Cina

Per le informazioni più recenti, consulta Differenze nella disponibilità e nell'implementazione delle funzionalità.

GuardDuty azioni e parametri precedenti

Amazon GuardDuty ha reso obsolete alcune azioni e parametri dell'API, ma le supporta ancora. La best practice consiste nell'utilizzare le nuove azioni e parametri API che sostituiscono le opzioni legacy. Nella tabella seguente vengono confrontate le operazioni e i parametri legacy e quelli nuovi.

Operazioni/parametri legacy	Operazioni/parametri nuovi	Confronto
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	Con la stessa implementazione in entrambe le azioni, GuardDuty utilizza il termine in. `Administrator` `DisassociateFromAdministratorAccount`
`autoEnable` parametro in DescribeOrganizationConfiguratione UpdateOrganization Configuration	`autoEnableOrganizationMembers`	Con`autoEnableOrganizationMembers`, l'account GuardDuty amministratore può controllare e applicare GuardDuty per tutti gli account membri uno dei valori. Utilizzando le API, l'aggiornamento della configurazione per tutti gli account membri può richiedere fino a 24 ore. Per ulteriori informazioni sui possibili valori del `autoEnableOrganizationMembers` campo, vedi Membri autoEnableOrganization
Parametro `dataSources` nelle API elencate in GuardDuty Modifiche alle	`features`	A partire da marzo 2023, puoi configurare Protezione da malware in Amazon GuardDuty e utilizzare i nuovi piani di GuardDuty protezion `efeatures`. I piani di protezione lanciati prima di marzo 2023, inclusa la protezione da malware, supportano ancora la configurazione tramite

Operazioni/ parametri legacy	Operazioni/parametri nuovi	Confronto
API a marzo 2023.		`dataSources` . Se utilizzi le API per configurare un piano di protezione, ogni richiesta API può includere `dataSources` o `features`, non entrambe.

Cronologia dei documenti per Amazon GuardDuty

La tabella seguente descrive importanti modifiche alla documentazione dall'ultima versione della Amazon GuardDuty User Guide. Per ricevere notifiche sugli aggiornamenti di questa documentazione, puoi abbonarti a un feed RSS.

Modifica	Descrizione	Data
Esperienza di console aggiornata per configurare l'esportazione dei risultati	GuardDuty ha aggiornato l'esperienza della console per esportare i risultati generati nel tuo Account AWS bucket Amazon S3. Per ulteriori informazioni, consulta Esportazione GuardDuty dei risultati.	1 aprile 2024
Funzionalità aggiornata in Runtime Monitoring	Runtime Monitoring ha rilasciato una nuova versione del security agent 1.1.0 per la risorsa Amazon EC2. Questa versione supporta la configurazione GuardDuty automatica degli agenti in Runtime Monitoring per le istanze Amazon EC2. Per informazioni sulle note di rilascio, consulta GuardDuty Security Agent for Amazon EC2 instance.	28 marzo 2024
Disponibilità generale del Runtime Monitoring per le istanze Amazon EC2	GuardDuty annuncia la disponibilità generale (GA) di Runtime Monitoring per le istanze Amazon EC2. Ora hai la possibilità di abilitare la configurazione automatizzata dell'agente che consente	28 marzo 2024

GuardDuty di installare e gestire l'agente di sicurezza per le tue istanze Amazon EC2 per tuo conto. Con l'agente GuardDuty automatizzato, puoi anche utilizzare tag di inclusione o esclusione e GuardDuty per informare sull'installazione e sulla gestione del security agent solo su istanze Amazon EC2 selezionate. Per ulteriori informazioni, consulta Come funziona il monitoraggio del runtime con le istanze Amazon EC2.

Elenco dei nuovi tipi di ricerca rilasciati insieme a questa GA

- Esecuzione: Runtime/SuspiciousTool
- Esecuzione: Runtime/SuspiciousCommand
- DefenseEvasionEsecuzione: Runtime/ ----sep----:runtime/SuspiciousCommand
- DefenseEvasion:Runtime/ ----Sep----:Runtime/PtraceAntiDebugging
- Esecuzione: Runtime/MaliciousFileExecuted

Amazon GuardDuty ha aggiornato il ruolo collegato ai servizi (SLR)	Usa AWS Systems Manager le azioni per gestire le associazioni SSM sulle istanze Amazon EC2 quando GuardDuty abiliti il monitoraggio del runtime con agente automatizzato per Amazon EC2. Quando la configurazione GuardDuty automatizzata degli agenti è disabilitata, GuardDuty considera solo le istanze EC2 che hanno un tag di inclusione (:). `GuardDutyManaged` `true` • L'elenco seguente mostra le nuove autorizzazioni: `"ssm:DescribeAssociation", "ssm:DeleteAssociation", "ssm:UpdateAssociation", "ssm:CreateAssociation", "ssm:StartAssociationsOnce", "ssm:AddTagsToResource", "ssm:CreateAssociation", "ssm:UpdateAssociation", "ssm:SendCommand", "ssm:GetCommandInvocation"`	26 marzo 2024

Funzionalità aggiornata in Runtime Monitoring	Con l'ultima versione GuardDuty di Security Agent (add-on) v1.5.0 per Amazon EKS, Runtime Monitoring ora supporta la configurazione di parametri specifici del tuo GuardDuty security agent, come impostazioni di CPU e memoria, impostazioni e impostazioni dei `PriorityClass` criteri DNS. Per ulteriori informazioni, consulta Configurazione dei parametri dell'agente di GuardDuty sicurezza (componente aggiuntivo EKS).	7 marzo 2024
Funzionalità aggiornata in Runtime Monitoring	Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.5.0 per le risorse Amazon EKS. Per informazioni sulle note di rilascio, consulta la cronologia dei rilasci dell'agente aggiuntivo EKS.	7 marzo 2024
Supporto per Canada West (Calgary)	Amazon GuardDuty è ora disponibile nella regione Canada occidentale (Calgary). Alcuni dei piani di protezione inclusi GuardDuty potrebbero non essere disponibili in questa regione. Per le informazioni più recenti, consulta Regioni ed endpoint.	6 marzo 2024

Funzionalità aggiornata in Runtime Monitoring	Le versioni GuardDuty di security agent 1.0.0 e 1.1.0 per i cluster Amazon EKS non saranno più supportate a partire dal 14 maggio 2024. Per informazioni sui passaggi da eseguire prima della fine del supporto standard, consulta l'agente di GuardDuty sicurezza per i cluster Amazon EKS.	16 febbraio 2024
Funzionalità aggiornata in Runtime Monitoring	Runtime Monitoring supporta l'ultima versione di Kubernetes 1.29 con la versione 1.4.1 del Security Agent esistente . Il supporto è disponibile dal lancio di questa versione di Kubernetes. Per informazioni sulle versioni di Kubernetes supportate, consulta Versioni di Kubernetes supportate dal security agent. GuardDuty	16 febbraio 2024

Funzionalità aggiornata in Runtime Monitoring - Disponibilità regionale	GuardDuty Il Runtime Monitoring ora supporta Amazon VPC condiviso all'interno dello stesso. AWS OrganizationsGuardDuty service-linked role (SLR) ha una nuova autorizzazione, `organizations:DescribeOrganization` che aiuta a recuperare l'ID dell'organizzazione per l'account Amazon VPC condiviso per impostare la policy degli endpoint. Per informazioni sui prerequisiti per l'utilizzo di un endpoint Amazon VPC condiviso in Runtime Monitoring, consulta Supporto per Amazon VPC condiviso. Questa funzionalità è disponibile in tutte le regioni in cui GuardDuty supporta il monitoraggio del runtime.	12 febbraio 2024

Funzionalità aggiornata in Runtime Monitoring - Disponibilità regionale	GuardDuty Il Runtime Monitoring ora supporta Amazon VPC condiviso all'interno dello stesso. AWS OrganizationsGuardDuty service-linked role (SLR) ha una nuova autorizzazione, `organizations:DescribeOrganization` che aiuta a recuperare l'ID dell'organizzazione per l'account Amazon VPC condiviso per impostare la policy degli endpoint. Per informazioni sui prerequisiti per l'utilizzo di un endpoint Amazon VPC condiviso in Runtime Monitoring, consulta Supporto per Amazon VPC condiviso. Attualmente, questa funzionalità è disponibile in alcuni dei. Regioni AWS Per ulteriori informazioni, consulta Regioni ed endpoint.	9 febbraio 2024
Funzionalità aggiornata con supporto per la nuova funzionalità Regioni AWS : Malware Protection	Malware Protection ora supporta la scansione dei volumi EBS crittografati con Chiavi gestite da AWS nella regione Stati Uniti occidentali (Oregon).	6 febbraio 2024

Funzionalità aggiornata con supporto per la nuova funzionalità Regioni AWS : Malware Protection	Malware Protection ora supporta la scansione dei volumi EBS crittografati con Chiavi gestite da AWS nei seguenti modi: Regioni AWS • Asia Pacifico (Singapore) (`ap-southeast-1`) • Europa (Francoforte) (`eu-central-1`) • Asia Pacifico (Osaka-Locale) (`ap-northeast-3`) • Stati Uniti orientali (Ohio) (`us-east-2`) • Europa (Milano) (`eu-south-1`) • Asia Pacifico (Tokyo) (`ap-northeast-1`) • Asia Pacifico (Seoul) (`ap-northeast-2`) • Canada (Centrale) (`ca-central-1`) • Europa (Irlanda) (`eu-west-1`) • Stati Uniti orientali (Virginia settentrionale) (`us-east-1`)	5 febbraio 2024

Funzionalità aggiornata in Runtime Monitoring	GuardDuty Runtime Monitoring ha rilasciato una nuova versione del GuardDuty security agent (v1.0.2) per le istanze Amazon EC2. Questa versione agente include il supporto per le AMI Amazon ECS più recenti. Per ulteriori informazioni sulla cronologia dei rilasci degli agenti, consulta GuardDuty Security Agent for Amazon EC2 Instances.	2 febbraio 2024

Funzionalità aggiornata con supporto per la nuova funzionalità Regioni AWS : Malware Protection	Malware Protection ora supporta la scansione dei volumi Amazon EBS crittografati con Chiavi gestite da AWS nei seguenti modi: Regioni AWS • Europa (Londra) (`eu-west-2`) • Europa (Stoccolma) (`eu-north-1`) • Asia Pacifico (Hong Kong) (`ap-east-1`) • Africa (Città del Capo) (`af-south-1`) • Medio Oriente (Bahrein) (`me-south-1`) • Asia Pacifico (Hyderabad) (`ap-south-2`) • Europa (Spagna) (`eu-south-2`) • Asia Pacifico (Melbourne) (`ap-southeast-4`) • Asia Pacifico (Sydney) (`ap-southeast-2`) • Israele (Tel Aviv) (`il-central-1`)	31 gennaio 2024

Aggiornamento: Gestione degli account con AWS Organizations	È stato riorganizzato il contenuto in Gestione degli account con AWS Organizations. , ha aggiunto la procedura per modificare l'account GuardDuty amministratore delegato e aggiornato Comprensione della relazione tra account GuardDuty amministratore e account membro.	30 gennaio 2024
Funzionalità aggiornata con supporto per nuove Regioni AWS	Malware Protection ora supporta la scansione dei volumi EBS crittografati con Chiavi gestite da AWS nei seguenti modi: Regioni AWS • Asia Pacifico (Giacarta) (`ap-southeast-3`) • Stati Uniti occidentali (California settentrionale) (`us-west-1`) • Medio Oriente (EAU) (`me-central-1`) • Europa (Zurigo) (`eu-central-2`) • Asia Pacifico (Mumbai) (`ap-south-1`) • Sud America (San Paolo) (`sa-east-1`)	29 gennaio 2024

Funzionalità aggiornate in Malware Protection	Malware Protection ora supporta la scansione dei volumi EBS crittografati utilizzando Chiavi gestite da AWS. Il ruolo collegato al servizio di Malware Protection (SLR) dispone di due nuove autorizzazioni: e. `GetSnapshotBlock` `ListSnapshotBlocks` Queste autorizzazioni consentiranno di GuardDuty recuperare l'istantanea di un volume EBS (con crittografia Chiave gestita da AWS) dall'utente Account AWS e copiarla sull'account del servizio GuardDuty prima di avviare la scansione antimalware. Attualmente, questa funzionalità è disponibile solo in Europa (Parigi) (). `eu-west-3` Per ulteriori informazioni, vedere Volumi supportati per la scansione antimalware.	25 gennaio 2024

Funzionalità aggiornata in Runtime Monitoring	GuardDuty Runtime Monitoring ha rilasciato una nuova versione del GuardDuty Security Agent (v1.0.1) con ottimizzazione e miglioramenti generali delle prestazioni. Per ulteriori informazioni sulla cronologia dei rilasci degli agenti, consulta GuardDuty Security Agent for Amazon EC2 Instances.	23 gennaio 2024
Funzionalità aggiornate in Runtime Monitoring	Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.4.1 per le risorse Amazon EKS. Per ulteriori informazioni, consulta Cronologia delle versioni dell'agente (componente aggiuntivo EKS).	16 gennaio 2024
Runtime Monitoring ha rilasciato il nuovo agente v1.4.0 per le risorse Amazon EKS	Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.4.0 per le risorse Amazon EKS. Per ulteriori informazioni, consulta Cronologia delle versioni dell'agente (componente aggiuntivo EKS).	21 dicembre 2023

Aggiunti tipi di risultati basati su S3 e AWS CloudTrail machine learning (ML) in Europa (Zurigo), Europa (Spagna), Asia Pacifico (Hyderabad), Asia Pacifico (Melbourne) e Israele (Tel Aviv)	Il seguente S3 e CloudTrail i risultati che identificano il comportamento anomalo utilizzando il modello GuardDuty di machine learning (ML) di rilevamento delle anomalie sono ora disponibili nelle regioni di Europa (Zurigo), Europa (Spagna), Asia Pacifico (Hyderabad), Asia Pacifico (Melbourne) e Israele (Tel Aviv): • 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	21 dicembre 2023

	• Persistence:IAMUser/AnomalousBehavior • PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty supporta 50.000 account membri tramite AWS Organizations	Un GuardDuty amministratore delegato può ora gestire un massimo di 50.000 account membri tramite. AWS Organizations Ciò include anche un massimo di 5000 account membri associati all'account GuardDuty amministratore tramite invito.	20 dicembre 2023
GuardDuty Il supporto per il monitoraggio del runtime è stato esteso a 19 Regioni AWS	Runtime Monitoring è ora disponibile in Asia Pacifico (Giacarta), Europa (Parigi), Asia Pacifico (Osaka), Asia Pacifico (Seoul), Medio Oriente (Bahrain), Europa (Spagna), Asia Pacifico (Hyderabad), Asia Pacifico (Melbourne), Israele (Tel Aviv), Stati Uniti occidentali (California settentrionale), Europa (Londra), Asia Pacifico (Hong Kong), Europa (Milano), Medio Oriente (Emirati Arabi Uniti)), Sud America (San Paolo), Asia Pacifico (Mumbai), Canada (Centrale), Africa (Città del Capo), Europa (Zurigo).	6 dicembre 2023

GuardDuty espande la funzionalità di monitoraggio del runtime	Oltre a rilevare le minacce ai cluster Amazon EKS, GuardDuty annuncia la disponibilità generale di Runtime Monitoring per rilevare le minacce ai carichi di lavoro Amazon ECS e una versione di anteprima per rilevare le minacce alle istanze Amazon EC2. Per ulteriori informazioni su quali Regioni AWS attualmente supportano il Runtime Monitoring, consulta Regioni ed endpoint.	26 novembre 2023

Amazon GuardDuty ha aggiornato il ruolo collegato ai servizi (SLR)	GuardDuty ha aggiunto nuove autorizzazioni per utilizzare le azioni Amazon ECS per gestire e recuperare informazioni sui cluster Amazon ECS e gestire le impostazioni dell'account Amazon ECS con. `guarddutyActivate` Le azioni relative ad Amazon ECS recuperano anche le informazioni sui tag associati a. GuardDuty • Le seguenti autorizzazioni sono state aggiunte come parte dell' GuardDuty espansione della funzionalità di monitoraggio del runtime: `"ecs:ListClusters", "ecs:DescribeClusters", "ecs:PutAccountSettingDefault"`	26 novembre 2023
Sono state aggiornate le politiche AWS gestite	GuardDuty ha aggiunto una nuova autorizzazione, `organizations:ListAccounts` alla AmazonGuardDutyFullAccessPolicyfine AmazonGuardDutyReadOnlyAccess.	16 novembre 2023

GuardDuty ha rilasciato nuovi tipi di risultati che utilizzano EKS Audit Log Monitoring.	EKS Audit Log Monitoring ora supporta i seguenti tipi di risultati in Asia Pacifico (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	11 novembre 2023

GuardDuty ha rilasciato nuovi tipi di risultati che utilizzano EKS Audit Log Monitoring.	EKS Audit Log Monitoring ora supporta i seguenti tipi di ricerca nelle regioni Asia Pacifico (Hyderabad) (`ap-south-2`), Europa (Zurigo) (`eu-central-2`) ed Europa (Spagna) (`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	10 novembre 2023

- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

GuardDuty ha rilasciato nuovi tipi di risultati che utilizzano EKS Audit Log Monitoring.	EKS Audit Log Monitoring ora supporta i seguenti tipi di risultati. Questi tipi di risultati non sono ancora disponibili nelle regioni Asia Pacifico (Hyderabad`ap-south-2`) (), Europa (Zurigo) (`eu-central-2`), Europa (Spagna) (`eu-south-2`) e Asia Pacifico (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	8 novembre 2023

	• PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	
Il monitoraggio del runtime EKS ha rilasciato il nuovo agente v1.3.1	EKS Runtime Monitoring ha rilasciato una nuova versione 1.3.1 dell'agente che include importanti patch e aggiornamenti di sicurezza.	23 ottobre 2023
Nuovo attributo del filtro per gli esiti	GuardDuty ha aggiunto nuovi criteri per filtrare i risultati generati. Il suffisso del dominio di richiesta DNS fornisce il dominio di secondo e primo livello coinvolto nell'attività che ha richiesto GuardDuty la generazione del risultato.	17 ottobre 2023
Il monitoraggio del runtime EKS ha rilasciato il nuovo agente v1.3.0 che supporta la versione 1.28 di Kubernetes	EKS Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.3.0 che supporta la versione 1.28 di Kubernetes. È stato aggiunto il supporto per Ubuntu. Per ulteriori informazioni, consulta Cronologia delle versioni dell'agente (componente aggiuntivo EKS).	5 ottobre 2023

Aggiunti tipi di risultati basati su S3 e AWS CloudTrail machine learning (ML) alle regioni Asia Pacifico (Giacarta) e Medio Oriente (Emirati Arabi Uniti)	Le seguenti informazioni su S3 e CloudTrail i risultati che identificano il comportamento anomalo utilizzando il modello GuardDuty di apprendimento automatico per il rilevamento delle anomalie (ML) sono ora disponibili nelle regioni di Asia Pacifico (Giacarta) e Medio Oriente (Emirati Arabi Uniti): • 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	20 settembre 2023

	• PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty EKS Runtime Monitoring introduce la gestione dell'agente di sicurezza a livello di cluster GuardDuty	EKS Runtime Monitoring aggiunge il supporto per la gestione dell'agente di GuardDuty sicurezza per i singoli cluster EKS per monitorare gli eventi di runtime solo da questi cluster selettivi . Il monitoraggio del runtime EKS estende questa funzionalità aggiungendo il supporto di tag.	13 settembre 2023
GuardDuty Malware Protection estende il supporto a molti altri Regioni AWS	La protezione da malware è ora disponibile in Asia Pacifico (Hyderabad), Asia Pacifico (Melbourne), Europa (Zurigo) ed Europa (Spagna).	11 settembre 2023

GuardDuty è ora disponibile nella regione di Israele (Tel Aviv)	È stata aggiunta la regione di Israele (Tel Aviv) all'elenco dei paesi Regioni AWS in cui GuardDuty è ora disponibile. I seguenti piani di protezione sono disponibili anche nella regione Israele (Tel Aviv): • GuardDuty Protezione EKS include il monitoraggio dei log di audit EKS e il monitoraggio del runtime EKS. • GuardDuty Protezione Lambda. • GuardDuty Protezione da malware. • GuardDuty Protezione S3. Per ulteriori informazioni sulla disponibilità del piano di protezione nella regione Israele (Tel Aviv), consulta Regioni ed endpoint.	24 agosto 2023
GuardDuty aggiunta della configurazione di attivazione automatica per l'organizzazione a livello di piano di protezione	Aggiorna la configurazione dell'organizzazione per i piani di protezione nella tua regione. Le opzioni di configurazione possibili sono: abilitazione per tutti gli account, abilitazione automatica per i nuovi account o abilitazione automatica disattivata per tutti gli account dell'organizzazione.	16 agosto 2023

I tipi di ricerca S3 che identificano comportamenti anomali utilizzando il modello GuardDuty di machine learning (ML) per il rilevamento delle anomalie sono ora disponibili in Asia Pacifico (Osaka)	I seguenti tipi di esiti sono ora disponibili nella regione Asia Pacifico (Osaka-Locale): • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	10 agosto 2023
Il monitoraggio del runtime EKS è ora disponibile in Asia Pacifico (Melbourne)	EKS Runtime Monitoring all'interno di GuardDuty EKS Protection fornisce il rilevamento delle minacce di runtime per i cluster Amazon EKS nell' AWS ambiente. Ora è disponibile nella regione Asia Pacifico (Melbourne).	8 agosto 2023
È stato aggiornato l'elenco dei GuardDuty risultati che richiamano la scansione antimalware GuardDuty avviata	Alcuni tipi di risultati di EKS Runtime Monitoring possono ora richiamare la scansione GuardDuty antimalware avviata nel tuo. Account AWS	19 luglio 2023

GuardDuty supporta 10.000 account membri tramite AWS Organizations	Un account GuardDuty amministratore può ora gestire un massimo di 10.000 account membri tramite AWS Organizations. Ciò include anche un massimo di 5000 account membri associati all'account GuardDuty amministratore su invito.	29 giugno 2023
Il monitoraggio del runtime EKS annuncia tre nuovi tipi di esiti.	Il monitoraggio del runtime EKS supporta tre nuovi tipi di esiti basati sulla tecnica di iniezione del processo. I nuovi tipi di ricerca sono:Runtime/ DefenseEv asion .Proc ,:Runtime/ ProcessInjection .Ptrace e:Runtime/. DefenseEvasion ProcessInjection DefenseEv asion ProcessInjection VirtualMemoryWrite.	22 giugno 2023
Il monitoraggio del runtime EKS ha rilasciato il nuovo agente v1.2.0 che supporta la versione 1.27 di Kubernetes	EKS Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.2.0 che supporta anche istanze basate su ARM64. È stato aggiunto il supporto per Bottlerocket. Per ulteriori informazioni, consulta Cronologia delle versioni dell'agente (componente aggiuntivo EKS).	16 giugno 2023

GuardDuty la console fornisce una visualizzazione riepilogativa dei risultati.	La dashboard di riepilogo nella GuardDuty console fornisce una visualizzazione aggregata dei GuardDuty risultati. Attualmente, la dashboard mostra i dati tramite vari widget per gli ultimi 10.000 risultati generati per il tuo account (o per gli account membro se sei un account GuardDuty amministratore) per la regione corrente.	12 giugno 2023
Il monitoraggio dei log di audit EKS è ora disponibile in Asia Pacifico (Hyderabad), Asia Pacifico (Melbourne), Europa (Zurigo) ed Europa (Spagna)	Abilita il monitoraggio dei log di audit EKS (nella Protezione EKS) per i tuoi account per monitorare i log di audit di Kubernetes dai cluster Amazon EKS e analizzarli per individuare attività potenzialmente dannose e sospette.	1 giugno 2023
Il monitoraggio dei log di audit EKS è ora disponibile in Medio Oriente (EAU)	EKS Audit Log Monitoring è ora disponibile in Medio Oriente (Emirati Arabi Uniti). Abilita il monitoraggio dei log di audit EKS per i tuoi account per monitorare i log di audit di Kubernetes dai cluster Amazon EKS e analizzarli per individuare attività potenzialmente dannose e sospette.	3 maggio 2023

GuardDuty Malware Protection annuncia la scansione antimalware su richiesta	La protezione da malware è utile per rilevare la presenza potenziale di malware nei volumi Amazon EBS collegati alle istanze Amazon EC2 e ai carichi di lavoro di un container. Ora offre due tipi di scansioni: GuardDuty avviate e su richiesta. GuardDuty -initiated malware scan avvia automaticamente una scansione senza agente nei volumi Amazon EBS solo quando GuardDuty genera uno dei Findings che richiamano la scansione antimalware avviata dall'utente. GuardDuty Puoi avviare una scansione antimalware on demand per le istanze Amazon EC2 nel tuo account fornendo il nome della risorsa Amazon (ARN) associato all'istanza Amazon EC2 in questione. Per ulteriori informazioni sulle differenze tra i due tipi di scansione, consulta Protezione da malware. • GuardDuty-scansione antimalware avviata • Scansione antimalware on demand	27 aprile 2023

GuardDuty annuncia Lambda Protection	La Protezione Lambda è utile per identificare potenziali minacce alla sicurezza nelle tue funzioni AWS Lambda . • Tipi di esiti della Protezione Lambda • Correzione di una funzione Lambda potenzialmente compromessa	20 aprile 2023
GuardDuty è ora disponibile nella regione Asia Pacifico (Melbourne)	È stata aggiunta l'area Asia Pacifico (Melbourne) all'elenco delle aree Regioni AWS in cui GuardDuty è disponibile. Per informazioni sulle funzionalità disponibili in questa regione, consulta Regioni ed endpoint.	19 aprile 2023
GuardDuty sono stati aggiunti 3 nuovi tipi di risultati EC2	GuardDuty introduce nuovi tipi di ricerca per rilevare l'uso di resolver DNS esterni e tecnologie DNS crittografate. Per informazioni su Regioni AWS dove sono supportati questi tipi di ricerca, consulta Regioni ed endpoint. • DefenseEvasion:EC2/UnusualDNSResolver • DefenseEvasion:EC2/UnusualDoHActivity • DefenseEvasion:EC2/UnusualDoTActivity	5 aprile 2023

GuardDuty annuncia EKS Runtime Monitoring in EKS Protection	EKS Runtime Monitoring all'interno di EKS Protection fornisce il rilevamento delle minacce di runtime per i cluster Amazon EKS nell' AWS ambiente. Viene utilizzato un agente (componente aggiuntivo di Amazon EKS, `aws-guardduty-agent`) che raccoglie gli Eventi di runtime dai carichi di lavoro EKS. Dopo aver GuardDuty ricevuto questi eventi di runtime, li monitora e li analizza per identificare potenziali minacce sospette alla sicurezza. Per ulteriori informazioni, consulta Dettagli sui risultati e Tipi di esiti del monitoraggio del runtime EKS.	30 marzo 2023

GuardDuty aggiunge una nuova funzionalità: `autoEnableOrganizationMembers`	Amazon GuardDuty aggiunge una nuova opzione di configurazione dell'organizzazione che aiuta a controllare e applicare gli account degli GuardDuty amministratori (se necessario) GuardDuty abilitata per `ALL` i membri dell'organizzazione. La best practice consiste ora nell'utilizzare `autoEnableOrganizationMembers` invece di `autoEnable` . L'opzione `autoEnable` è obsoleta, ma è ancora supportata. Questa nuova funzionalità ha un impatto sulle API seguenti: • DescribeOrganizationConfiguration • UpdateOrganizationConfiguration • DisassociateMembers • DeleteMembers • DisassociateFromAdministratorAccount • StopMonitoringMembers	23 marzo 2023

La funzionalità RDS Protection in Amazon GuardDuty è ora disponibile a livello generale	GuardDuty RDS Protection monitora e profila l'attività di accesso RDS per identificare comportamenti di accesso sospetti sulle istanze del database Amazon Aurora. Per informazioni sulle Regioni AWS che supportano la Protezione RDS, consulta Regioni ed endpoint.	16 marzo 2023
GuardDuty annuncia l'attivazione della funzionalità	In passato, l' GuardDuty API consentiva la configurazione sia delle funzionalità che delle fonti di dati, ma ora tutti i nuovi tipi di GuardDuty protezione verranno configurati come funzionalità e non come fonti di dati. GuardDuty supporta ancora le fonti di dati tramite API ma non aggiungerà una nuova API. L'attivazione delle funzionalità influisce sul comportamento delle API utilizzate per abilitare GuardDuty o su un tipo di protezione all'interno GuardDuty. Se gestisci i tuoi GuardDuty account tramite API, SDK o modello CFN, consulta le modifiche all'GuardDuty API di marzo 2023.	16 marzo 2023

GuardDuty La protezione da malware è ora disponibile nella regione del Medio Oriente (Emirati Arabi Uniti)	La funzionalità Malware Protection in GuardDuty è supportata nella regione del Medio Oriente (Emirati Arabi Uniti). Per ulteriori informazioni, consulta Regioni ed endpoint.	13 marzo 2023
Amazon GuardDuty ha aggiornato il ruolo collegato ai servizi (SLR)	GuardDuty ha aggiunto le seguenti nuove autorizzazioni per supportare la prossima funzionalità GuardDuty EKS Runtime Monitoring. • Utilizza le operazioni di Amazon EKS per gestire e recuperare informazioni sui cluster EKS e gestisci i componenti aggiuntivi EKS su questi cluster. Le azioni EKS recuperano anche le informazioni sui tag associati a. GuardDuty `"eks:ListClusters", "eks:DescribeCluster", "ec2:DescribeVpcEndpointServices", "ec2:DescribeSecurityGroups"`	8 marzo 2023
Amazon GuardDuty ha aggiornato il ruolo collegato ai servizi (SLR)	La GuardDuty SLR è stata aggiornata per consentire la creazione di Malware Protection SLR dopo l'attivazione di Malware Protection.	21 febbraio 2023

GuardDuty richiede TLS v1.2 o versione successiva	Per comunicare con AWS le risorse, GuardDuty richiede e supporta TLS v1.2 o versione successiva. Per ulteriori informazioni, consulta Protezione dei dati e Sicurezza dell'infrastruttura.	14 febbraio 2023
GuardDuty è ora disponibile nella regione Asia Pacifico (Hyderabad)	È stata aggiunta la regione Asia Pacifico (Hyderabad) all'elenco delle Regioni AWS aree in cui è disponibile. GuardDuty Per ulteriori informazioni, consulta Regioni ed endpoint.	14 febbraio 2023
Amazon GuardDuty User Guide è in linea con le best practice IAM	Guida aggiornata per l'allineamento alle best practice IAM. Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.	10 febbraio 2023
GuardDuty è ora disponibile nella regione Europa (Spagna)	È stata aggiunta l'Europa (Spagna) all'elenco dei paesi Regioni AWS in cui GuardDuty è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint.	8 febbraio 2023
GuardDuty è ora disponibile nella regione Europa (Zurigo)	È stata aggiunta Europa (Zurigo) all'elenco dei paesi Regioni AWS in cui GuardDuty è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint.	12 dicembre 2022

Versione di anteprima di una nuova funzionalità: GuardDuty RDS Protection	GuardDuty RDS Protection monitora e profila l'attività di accesso RDS per identificare comportamenti di accesso sospetti sulle istanze del database Amazon Aurora. Attualmente, è disponibile per una versione di anteprima in cinque Regioni AWS. Per ulteriori informazioni, consulta Regioni ed endpoint.	30 novembre 2022
GuardDuty è ora disponibile nella regione del Medio Oriente (Emirati Arabi Uniti)	È stato aggiunto il Medio Oriente (Emirati Arabi Uniti) all'elenco delle aree Regioni AWS in cui GuardDuty è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint.	6 ottobre 2022

Contenuto aggiunto per una nuova funzionalità: GuardDuty Malware Protection	GuardDuty La protezione da malware è un miglioram ento opzionale di Amazon. GuardDuty Oltre a GuardDuty identificare le risorse a rischio, Malware Protectio n rileva il malware che potrebbe essere all'origine della compromissione. Con Malware Protection abilitata , ogni volta che GuardDuty rileva un comportamento sospetto su un'istanza Amazon EC2 o un carico di lavoro di container indicativ o di malware GuardDuty , Malware Protection avvia una scansione senza agente sui volumi EBS collegati ai carichi di lavoro delle istanze EC2 o dei container interessati per rilevare la presenza di malware. Per informazioni sul funzionamento di Malware Protection e sulla configura zione di questa funzionalità, consulta Malware Protection. GuardDuty • Per informazioni sugli esiti della protezione da malware, consulta Dettagli sui risultati. • Per informazioni sulla riparazione dell'istanza EC2 compromessa e di	26 luglio 2022

	un contenitore autonomo, consulta Risolvere i problemi di sicurezza rilevati da. GuardDuty • Per informazioni sul controllo dei CloudWatch log per le scansioni antimalware e sui motivi per cui una risorsa viene ignorata durante la scansione antimalware, consulta Comprendere i log e ignorare i motivi. CloudWatch • Per informazioni sui rilevamenti di minacce false positive, consulta Segnalazione di falsi positivi in Malware Protection. GuardDuty	
È stato ritirato un tipo di esito	Exfiltration:S3/ObjectRead.Unusual è stato ritirato.	5 luglio 2022

Sono stati aggiunti nuovi tipi di ricerca S3 che identificano i comportamenti anomali utilizzando il modello di apprendimento automatico (ML) GuardDuty di rilevamento delle anomalie.	Sono stati aggiunti i nuovi tipi di esiti S3 seguenti. Questi tipi di esiti rilevano se una richiesta API ha richiamato un'entità IAM in modo anomalo. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Per ulteriori informazioni su ciascuno di questi nuovi esiti, consulta Tipi di esiti S3. • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	5 luglio 2022

Aggiunti contenuti GuardDuty di protezione EKS per GuardDuty	GuardDuty ora puoi generare risultati per le tue risorse Amazon EKS attraverso il monitoraggio dei log di audit di Kubernetes. Per informazioni su come configurare questa funzionalità, consulta EKS Protection in Amazon GuardDuty. Per un elenco dei risultati che è GuardDuty possibile generare per le risorse di Amazon EKS, consulta i risultati di Kubernetes. Sono state aggiunte nuove linee guida sulla correzione e di questi esiti nella Guida alla correzione degli esiti di Kubernetes.	25 gennaio 2022
È stato aggiunto un nuovo esito	È stato aggiunto un nuovo esito UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS. Questo risultato ti informa quando un account esterno al tuo ambiente accede alle credenziali dell'istanza. AWS AWS	20 gennaio 2022

Sono stati aggiornati i tipi di esiti utili per identificare i problemi relativi a log4j	Amazon GuardDuty ha aggiornato i seguenti tipi di risultati per aiutare a identificare e dare priorità ai problemi relativi a CVE-2021-44228 e CVE-2021-45046: Backdoor:EC2/C&CActivity.b; Backdoor:EC2/C&CActivity.b!NetworkPortUnusualDNS; comportamento: EC2/.	22 dicembre 2021
Modifiche agli esiti	UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration è stato modificato in UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS. Questa versione migliorata dell'esito rileva le posizioni da cui vengono solitamente utilizzate le credenziali, riducendo così gli esiti del traffico instradato attraverso le reti on-premise. UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	7 settembre 2021
Aggiornamento GuardDuty a SLR	La GuardDuty reflex è stata aggiornata con nuove azioni per migliorare la precisione di ricerca.	3 agosto 2021
Sono state aggiunte informazioni sull'origine dati per ogni tipo di esito.	Le descrizioni dei risultati ora contengono informazioni sulle fonti di dati GuardDuty utilizzate per generare tali risultati.	10 maggio 2021

Sono stati ritirati 13 tipi di esiti.	13 risultati sono stati ritirati per essere sostituiti con nuovi AnomalousBehavoir risultati. 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.UnusualImpact:S3/ObjectDelete.Unusual, Impact:S3/PermissionsModification.Unusual.	12 marzo 2021

Sono stati aggiunti 8 nuovi tipi di esiti per comportamenti anomali.	Sono stati aggiunti 8 nuovi tipi di esiti IAMUser basati sul comportamento anomalo per i principali 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 marzo 2021
Sono stati aggiunti alcuni esiti EC2 basati sulla reputazione del dominio.	Sono stati aggiunti 4 nuovi tipi di esiti Impatto basati sulla reputazione del dominio. Impact:EC2/AbusedDomainRequest.Reputation , Impact:EC2/BitcoinDomainRequest.Reputation, Impact:EC2/MaliciousDomainRequest.Reputation. È stato aggiunto anche un nuovo esito EC2 per C&CActivity. Impact:EC2/SuspiciousDomainRequest.Reputation	27 gennaio 2021

Sono stati aggiunti 4 nuovi tipi di esiti.	Sono stati aggiunti 3 nuovi esiti S3 MaliciousIPCaller. Discovery:S3/MaliciousIPCaller, Exfiltration:S3/MaliciousIPCaller, Impact:S3/MaliciousIPCaller. È stato aggiunto anche un nuovo esito EC2 per C&CActivity. Backdoor:EC2/C&CActivity.B	21 dicembre 2020
È stato ritirato il tipo di esito UnauthorizedAccess:EC2/TorIPCaller.	Il tipo di UnauthorizedAccess:EC2/TorIPCaller ricerca è stato ora GuardDuty ritirato. Ulteriori informazioni.	1 ottobre 2020
È stato aggiunto il tipo di esito Impact:EC2/WinRmBruteForce.	È stato aggiunto un nuovo esito Impatto, ossia Impact:EC2/WinRmBruteForce. Ulteriori informazioni.	17 settembre 2020
È stato aggiunto il tipo di esito Impact:EC2/PortSweep.	È stato aggiunto un nuovo esito Impatto, ossia Impact:EC2/PortSweep. Ulteriori informazioni.	17 settembre 2020
GuardDuty è ora disponibile nelle regioni Africa (Città del Capo) ed Europa (Milano).	Aggiunte Africa (Città del Capo) ed Europa (Milano) all'elenco delle AWS regioni in cui GuardDuty è disponibile. Ulteriori informazioni	31 luglio 2020

Sono stati aggiunti nuovi dettagli di utilizzo per il monitoraggio GuardDuty dei costi.	Ora puoi utilizzare nuove metriche per interrogare i dati sui costi di GuardDuty utilizzo per il tuo account e gli account che gestisci. È disponibile una nuova panoramica dei costi di utilizzo nella console all'indirizzo https://console.aws.amazon.com/guardduty/. È possibile accedere a informazioni più dettagliate tramite l'API.	31 luglio 2020
Sono stati aggiunti contenuti che coprono la protezione di S3 tramite il monitoraggio degli eventi dei dati di S3 in. GuardDuty	GuardDuty S3 Protection è ora disponibile tramite il monitoraggio degli eventi del piano dati S3 come nuova fonte di dati. Questa funzionalità sarà abilitata automaticamente per i nuovi account. Se lo stai già utilizzando, GuardDuty puoi abilitare la nuova fonte di dati per te o per i tuoi account membro.	31 luglio 2020
Sono stati aggiunti 14 nuovi esiti S3.	Sono stati aggiunti 14 nuovi tipi di esiti S3 per le origini del piano di controllo (control-plane) e del piano dati S3.	31 luglio 2020

È stato aggiunto il supporto per gli esiti S3 e sono stati modificati i nomi di 2 tipi di esiti esistenti.	GuardDuty i risultati ora includono maggiori dettagli sui risultati che coinvolgo no i bucket S3. I tipi di esiti esistenti correlati all'attività di S3 sono stati rinominati: Policy:IAMUser/S3BlockPubli cAccessDisabled è stato modificato in Policy:S3/ BucketBlockPublicAccessDis abled e Stealth:IAMUser/S3 ServerAccessLoggingDisabled è stato modificato in Stealth:S 3/ServerAccessLoggingDisabl ed.	28 maggio 2020
Contenuti aggiunti per l'integra zione AWS Organizations .	GuardDuty ora si integra con gli amministratori AWS Organizations delegati per consentirti di gestire gli GuardDuty account all'inter no della tua organizzazione. Quando imposti un amministr atore delegato come account GuardDuty amministratore, puoi abilitare automaticamente la gestione GuardDuty di qualsiasi membro dell'orga nizzazione da parte dell'acco unt amministratore delegato. È inoltre possibile abilitare automaticamente gli account GuardDuty dei nuovi AWS Organizations membri. Ulteriori informazioni.	20 aprile 2020

Sono stati aggiunti contenuti per la funzionalità di esportazione degli esiti.	Contenuto aggiunto che descrive la funzionalità Export Findings di GuardDuty.	14 novembre 2019
È stato aggiunto il tipo di esito UnauthorizedAccess:EC2/MetadataDNSRebind.	È stato aggiunto un nuovo esito Non autorizzato, ossia UnauthorizedAccess:EC2/MetadataDNSRebind. Ulteriori informazioni.	10 ottobre 2019
È stato aggiunto il tipo di esito Stealth:IAMUser/S3ServerAccessLoggingDisabled.	È stato aggiunto un nuovo esito Stealth, ossia Stealth:IAMUser/S3ServerAccessLoggingDisabled. Ulteriori informazioni.	10 ottobre 2019
È stato aggiunto il tipo di esito Policy:IAMUser/S3BlockPublicAccessDisabled.	È stato aggiunto un nuovo esito Policy, ossia Policy:IAMUser/S3BlockPublicAccessDisabled. Ulteriori informazioni.	10 ottobre 2019
È stato ritirato il tipo di esito Backdoor:EC2/XORDDOS.	Il tipo di Backdoor:EC2/XORDDOS risultato è stato ora ritirato da GuardDuty. Scopri di più	12 giugno 2019
È stato aggiunto il tipo di esito PrivilegeEscalation.	Il tipo di esito Privilege Escalation rileva quando gli utenti tentano di assegnare privilegi di escalation più permissivi ai loro account. Ulteriori informazioni	14 maggio 2019

GuardDuty è ora disponibile nella regione Europa (Stoccolma).	È stato aggiunto Europa (Stoccolma) all'elenco delle AWS regioni in cui GuardDuty è disponibile. Ulteriori informazioni	9 maggio 2019
È stato aggiunto un nuovo tipo di esito, ossia Recon:EC2/PortProbeEMRUnprotectedPort.	Questo risultato segnala che una porta sensibile correlata a EMR su un'istanza EC2 non è bloccata ed è sottoposta attivamente a probing. Ulteriori informazioni	8 maggio 2019
Sono stati aggiunti 5 nuovi tipi di esiti in grado di rilevare se le istanze EC2 vengono potenzialmente utilizzate per attacchi Denial of Service (DoS).	Questi risultati ti informano delle istanze EC2 nell'ambiente che si comportano in un modo che potrebbe indicare che vengono utilizzate per eseguire attacchi Denial of Service (DoS). Ulteriori informazioni	8 marzo 2019
È stato aggiunto un nuovo tipo di esito: Policy:IAMUser/RootCredentialUsage	Policy:IAMUser/RootCredentialUsagefinding type informa l'utente che le credenziali di accesso dell'utente root Account AWS vengono utilizzate per effettuare richieste programmatiche ai servizi. AWS Ulteriori informazioni	24 gennaio 2019

Il tipo di esito UnauthorizedAccess:IAMUser/UnusualASNCaller è stato ritirato	Il tipo di esito UnauthorizedAccess:IAMUser/UnusualASNCaller è stato ritirato. Ora riceverete una notifica sulle attività richiamate da reti insolite tramite altri tipi di ricerca attivi. GuardDuty Il tipo di ricerca generato sarà basato sulla categoria dell'API che è stata richiamata da una rete insolita. Ulteriori informazioni	21 dicembre 2018
Sono stati aggiunti due nuovi tipi di esiti: PenTest:IAMUser/ParrotLinux e PenTest:IAMUser/PentooLinux	I tipi di esiti PenTest:IAMUser/ParrotLinux segnalano che un computer su cui è in esecuzione Parrot Security Linux effettua chiamate API utilizzando credenziali che appartengono al tuo account AWS . I tipi di esiti PenTest:IAMUser/PentooLinux segnalano che una macchina su cui è in esecuzione Pentoo Linux effettua chiamate API utilizzando credenziali che appartengono al tuo account AWS . Ulteriori informazioni	21 dicembre 2018

È stato aggiunto il supporto per l'argomento GuardDuty SNS degli annunci di Amazon	Ora puoi iscriverti all'argomento « GuardDuty Annunci» su SNS per ricevere notifiche sui nuovi tipi di risultati rilasciati, aggiornamenti ai tipi di risultati esistenti e altre modifiche alle funzionalità. Le notifiche sono disponibili in tutti i formati supportati da Amazon SNS. Ulteriori informazioni	21 novembre 2018
Sono stati aggiunti due nuovi tipi di esiti: UnauthorizedAccess:EC2/TorClient e UnauthorizedAccess:EC2/TorRelay	UnauthorizedAccess:EC2/TorClientfinding type ti informa che un'istanza EC2 nel tuo AWS ambiente sta effettuando connessioni a un nodo Tor Guard o a un nodo Authority. UnauthorizedAccess:EC2/TorRelayfinding type ti informa che un'istanza EC2 nel tuo AWS ambiente sta effettuando connessioni a una rete Tor in un modo che suggerisce che stia agendo come un relè Tor. Ulteriori informazioni	16 novembre 2018
È stato aggiunto un nuovo tipo di esito: CryptoCurrency:EC2/BitcoinTool.B	Questa scoperta ti informa che un'istanza EC2 nel tuo AWS ambiente sta interrogando un nome di dominio associato a Bitcoin o ad altre attività legate alle criptovalute. Ulteriori informazioni	9 novembre 2018

È stato aggiunto il supporto per l'aggiornamento della frequenza delle notifiche inviate a Events CloudWatch	Ora puoi aggiornare la frequenza delle notifiche inviate a CloudWatch Events per le successive occorrenz e di risultati esistenti. I valori possibili sono 15 minuti, 1 ora o 6 ore (impostazione predefini ta). Ulteriori informazioni	9 ottobre 2018
È stato aggiunto il supporto per una regione	È stato aggiunto il supporto regionale per AWS GovCloud (Stati Uniti occidentali) Ulteriori informazioni	25 luglio 2018
È stato aggiunto il supporto per in AWS CloudFormation StackSets GuardDuty	Puoi utilizzare il GuardDuty modello Enable Amazon per eseguire l'attivazione GuardDuty simultanea in più account. Ulteriori informazioni	25 giugno 2018
Aggiunto il supporto per le regole di GuardDuty archiviaz ione automatica	I clienti possono ora creare regole di archiviazione automatica granulari per la soppressione dei risultati. I risultati che corrispondono a una regola di archiviazione automatica, li contrassegna GuardDuty automaticamente come archiviati. Ciò consente ai clienti di effettuare ulteriori ottimizzazioni GuardDuty per conservare solo i risultati pertinenti nella tabella dei risultati corrente. Ulteriori informazioni	4 maggio 2018

GuardDuty è disponibile nella regione Europa (Parigi)	GuardDuty è ora disponibile in Europa (Parigi) e consente di estendere il monitoraggio continuo della sicurezza e il rilevamento delle minacce in questa regione. Ulteriori informazioni	29 marzo 2018
AWS CloudFormation È ora supportata la creazione di account GuardDuty amministratore e account membro tramite.	Per ulteriori informazioni, consultare `AWS::GuardDuty::master` e `AWS::GuardDuty::member`.	6 marzo 2018
Sono stati aggiunti nove nuovi rilevamenti di anomalie CloudTrail basati.	Questi nuovi tipi di ricerca vengono abilitati automaticamente GuardDuty in tutte le regioni supportate. Ulteriori informazioni	28 febbraio 2018
Aggiunti tre nuovi tipi di rilevamento intelligente delle minacce (tipi di ricerca).	Questi nuovi tipi di ricerca vengono abilitati automaticamente GuardDuty in tutte le regioni supportate. Ulteriori informazioni	5 febbraio 2018
Aumento del limite per GuardDuty gli account dei membri.	Con questa versione, è possibile aggiungere fino a 1000 account GuardDuty membro per AWS account (account GuardDuty amministratore). Ulteriori informazioni	25 gennaio 2018

Modifiche al caricamento e ulteriore gestione degli elenchi di IP affidabili e degli elenchi di minacce per gli account GuardDuty amministratore e gli account dei membri.	Con questa versione, gli utenti degli GuardDuty account di amministratore possono caricare e gestire elenchi di IP affidabili ed elenchi di minacce. Gli utenti degli GuardDuty account membri non possono caricare e gestire elenchi. Gli elenchi di IP affidabili e gli elenchi di minacce caricati dall'account amministratore sono soggetti a restrizioni di GuardDuty funzionalità negli account dei membri. Ulteriori informazioni	25 gennaio 2018

Aggiornamenti precedenti

Modifica	Descrizione	Data
Pubblicazione iniziale	Pubblicazione iniziale della Amazon GuardDuty User Guide.	28 novembre 2017

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.