



AWS Security Incident Response Guida per l'utente



Version March 27, 2026

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

AWS Security Incident Response Guida per l'utente:

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

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

Table of Contents

Che cos'è AWS Security Incident Response?	1
Configurazioni supportate	1
Riepilogo delle funzionalità	3
Monitoraggio e indagine	3
Semplifica la risposta agli incidenti	3
Soluzioni di sicurezza self-service	3
Dashboard per la visibilità	3
Posizione di sicurezza	3
Assistenza rapida	4
Preparazione e prontezza	4
Concetti e terminologia	5
Nozioni di base	7
Guida all'imbarco	7
Implementa e configura Security Incident Response	9
Autorizza le azioni di monitoraggio e contenimento	11
Dopo l'implementazione di Security Incident Response	14
Aggiorna l'Incident Response Team	14
AWS caso supportato	15
GuardDuty risultati e regole di soppressione	17
Amazon EventBridge	18
Integrazioni e flusso di lavoro con strumenti esterni	20
Flusso di lavoro con utensili esterni	21
Appendice A: Punti di contatto	21
Matrice RACI	23
Seleziona un account di iscrizione	25
Configura i dettagli dell'iscrizione	27
Associa gli account a AWS Organizations	27
Imposta flussi di lavoro proattivi di risposta e valutazione degli avvisi	28
Comprendere l'archiviazione automatica con Proactive Response	28
Attività dell'utente	31
Pannello di controllo	31
Gestire il mio Incident Response Team	31
Preferenze di comunicazione	32
Associazione dell'account a AWS Organizations	34
Monitoraggio e indagine	3

Casi	50
Gestione dei casi	59
Lavorare con CloudFormation StackSets	64
Annulla iscrizione	71
Taggare le risorse AWS Security Incident Response	72
Usando AWS CloudShell	73
Ottenere le autorizzazioni IAM per AWS CloudShell	73
Interazione con Security Incident Response tramite AWS CloudShell	74
CloudTrail registri	75
Informazioni sulla risposta agli incidenti di sicurezza in CloudTrail	75
Informazioni sulle voci dei file di registro di Security Incident Response	77
Gestione degli account con AWS Organizations	80
Considerazioni e raccomandazioni	80
Accesso sicuro	81
Autorizzazioni necessarie per designare un account amministratore delegato di Security Incident Response	83
Designazione di un amministratore delegato AWS Security Incident Response	84
Gestione dell'appartenenza alle unità organizzative (OUs)	86
Aggiungere membri a AWS Security Incident Response	87
Rimozione di membri da AWS Security Incident Response	88
.....	89
Gestione degli eventi tramite EventBridge	89
Invio di eventi Security Incident Response	90
Riferimento ai dettagli sugli eventi	91
Eventi del caso	93
Eventi di commento al caso	96
Eventi per i soci	99
Utilizzo AWS Security Incident Response degli eventi	101
Tutorial: invio di avvisi Amazon Simple Notification Service per Membership Updated eventi	103
Prerequisiti	103
Tutorial: creare e sottoscrivere un argomento di Amazon SNS	103
Tutorial: Registra una regola di evento	104
Tutorial: verifica la tua regola	105
Regola alternativa: Security Incident Response Case Updates	106
Risoluzione dei problemi	107
Problemi	107

Errori	107
Supporto	108
Sicurezza	110
Protezione dei dati in AWS Security Incident Response	110
Crittografia dei dati	111
Riservatezza del traffico inter-rete	112
Traffico tra servizio e applicazioni e client locali	112
Traffico tra AWS risorse nella stessa regione	112
Identity and Access Management	113
Autenticazione con identità	114
Come AWS Security Incident Response funziona con IAM	117
Risoluzione dei problemi relativi a AWS Security Incident Response identità e accesso	124
Utilizzo dei ruoli di servizio	126
Uso di ruoli collegati ai servizi	126
AWSServiceRoleForSecurityIncidentResponse	127
AWSServiceRoleForSecurityIncidentResponse_Triage	128
Regioni supportate per SLRs	130
AWS Policy gestite	131
politica gestita: AWSSecurity IncidentResponseServiceRolePolicy	132
politica gestita: AWSSecurity IncidentResponseAdmin	133
politica gestita: AWSSecurity IncidentResponseReadOnlyAccess	133
politica gestita: AWSSecurity IncidentResponseCaseFullAccess	134
politica gestita: AWSSecurity IncidentResponseTriageServiceRolePolicy	135
Aggiornamenti SLRs e politiche gestite	136
Risposta agli incidenti	139
Convalida della conformità	140
Registrazione e monitoraggio in AWS Security Incident Response	141
Resilienza	141
Sicurezza dell'infrastruttura	142
Analisi della configurazione e delle vulnerabilità	142
Prevenzione del confused deputy tra servizi	142
Service Quotas	144
AWS Security Incident Response	144
AWS Security Incident Response Guida tecnica	145
Sintesi	145
Sei Well-Architected?	145
Introduzione	146

Prima di iniziare	146
AWS panoramica della risposta agli incidenti	147
Preparazione	153
Persone	154
Processo	158
Tecnologia	165
Riepilogo degli elementi di preparazione	173
Operazioni	178
Rilevamento	179
Analisi	183
Contenimento	188
Rimozione	194
Ripristino	196
Conclusioni	197
Attività post-incidente	199
Stabilire un quadro per imparare dagli incidenti	199
Stabilisci metriche per il successo	201
Usa indicatori di compromesso	204
Istruzione e formazione continue	205
Conclusioni	206
Collaboratori	206
Appendice A: Definizioni delle funzionalità cloud	206
Registrazione ed eventi	207
Visibilità e avvisi	209
Automazione	211
Archiviazione sicura	212
Funzionalità di sicurezza future e personalizzate	212
Appendice B: risorse per la risposta AWS agli incidenti	213
Risorse del playbook	213
Risorse forensi	213
Note	214
Cronologia dei documenti	215
.....	ccxxxii

Che cos'è AWS Security Incident Response?

AWS Security Incident Response ti aiuta a prepararti, rispondere e ricevere rapidamente indicazioni per aiutarti a riprenderti dagli incidenti di sicurezza. Ciò include incidenti come acquisizione di account, violazioni di dati e attacchi ransomware.

AWS Security Incident Response analizza le rilevazioni delle minacce, analizza gli eventi di sicurezza e gestisce i casi che richiedono la tua attenzione immediata. Inoltre, hai accesso ai tecnici del Security Incident Response, che esamineranno le risorse interessate.

Note

Non vi è alcuna garanzia che le risorse interessate possano essere recuperate. Consigliamo di creare e mantenere backup per le risorse che potrebbero influire sui requisiti aziendali.

AWS Security Incident Response funziona con altri servizi [AWS di rilevamento e risposta](#), guidandovi attraverso l'intero ciclo di vita degli incidenti, dal rilevamento al ripristino.

Indice

- [Configurazioni supportate](#)
- [Riepilogo delle funzionalità](#)

Configurazioni supportate

AWS Security Incident Response supporta le seguenti configurazioni di lingua e regione:

- **Lingua:** AWS Security Incident Response fornisce un supporto dedicato in inglese. Il supporto per la lingua giapponese è limitato all'orario lavorativo dell'ora solare del Giappone e prevede restrizioni specifiche:

Note

L'assistenza in lingua giapponese viene fornita con la massima diligenza possibile durante l'orario lavorativo (dalle 09:00 alle 17:00, dal lunedì al venerdì, esclusi i giorni festivi)

- **Regioni supportate:** AWS

AWS Security Incident Response è disponibile in un sottoinsieme di Regioni AWS. In queste regioni supportate, puoi creare un'iscrizione, creare e visualizzare casi e accedere alla dashboard.

- Stati Uniti orientali (Ohio)
- Stati Uniti occidentali (Oregon)
- Stati Uniti orientali (Virginia)
- Europa (Francoforte)
- Europa (Irlanda)
- Europa (Londra)
- Europa (Milano)
- Europa (Parigi)
- Europa (Spagna)
- Europa (Stoccolma)
- Europa (Zurigo)
- Asia Pacifico (Hong Kong)
- Asia Pacifico (Hyderabad)
- Asia Pacifico (Giacarta)
- Asia Pacifico (Melbourne)
- Asia Pacifico (Mumbai)
- Asia Pacifico (Seoul)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Tokyo)
- Canada (Centrale)
- Medio Oriente (Bahrein)
- Medio Oriente (Emirati Arabi Uniti)
- Sud America (San Paolo)
- Africa (Città del Capo)

Quando abiliti la funzionalità di monitoraggio e indagine, AWS Security Incident Response monitora i GuardDuty risultati di Amazon relativi a tutte le pubblicità Regioni AWS attive. Come best

Questa configurazione consente di GuardDuty generare informazioni su attività non autorizzate o

insolite, anche Regioni AWS laddove non si distribuiscono attivamente le risorse. In questo modo, migliorate il vostro livello di sicurezza generale e mantenete una copertura completa di rilevamento delle minacce in tutto l'ambiente. AWS

Note

Amazon GuardDuty riporta i risultati per le regioni configurate. Se scegli di non abilitare il servizio in una regione specifica, gli avvisi non saranno disponibili.

Riepilogo delle funzionalità

Monitoraggio e indagine

AWS Security Incident Response esamina rapidamente gli avvisi sulle minacce alla sicurezza provenienti da Amazon GuardDuty e dalle integrazioni di terze parti AWS Security Hub CSPM, riducendo il numero di dati che il team deve analizzare. Configura le regole di soppressione in base al tuo ambiente per ridurre gli avvisi di minaccia che devi valutare e indagare.

Semplifica la risposta agli incidenti

Ridimensiona ed esegui la risposta agli incidenti in pochi minuti con le parti interessate, i servizi e gli strumenti di terze parti.

Soluzioni di sicurezza self-service

AWS Security Incident Response fornisce APIs l'integrazione e consente di creare soluzioni di sicurezza personalizzate.

Dashboard per la visibilità

Monitora e misura la prontezza di risposta agli incidenti.

Posizione di sicurezza

Accedi alle AWS migliori pratiche e agli strumenti controllati per la valutazione della sicurezza e le indagini sulla risposta rapida agli incidenti.

Assistenza rapida

Connect con i tecnici di Security Incident Response per indagare, contenere e ricevere indicazioni sui modi per riprendersi dagli eventi di sicurezza.

Preparazione e prontezza

Implementa notifiche semplificate configurando il team Incident Response che attiva avvisi a individui o gruppi designati, con politiche di autorizzazione predefinite.

Concetti e terminologia

I termini e i concetti seguenti sono importanti per comprendere il AWS Security Incident Response servizio e il suo funzionamento.

Scopo: AWS Security Incident Response si allinea alla Guida 800-61 del National Institute of Standards and Technology (NIST) 800-61 sulla gestione degli incidenti di sicurezza informatica, che fornisce un approccio coerente alla gestione degli eventi di sicurezza in relazione alle migliori pratiche del settore.

Analisi: l'indagine e l'esame dettagliati di un evento di sicurezza per comprenderne la portata, l'impatto e la causa principale.

AWS Security Incident Response portale di assistenza: un portale self-service che consente di avviare e gestire casi di eventi di sicurezza. Comunicazione e reportistica continue agevolate dal sistema di biglietteria, dalle notifiche automatiche e dal coinvolgimento diretto con il team di assistenza.

Comunicazione: il dialogo continuo e la condivisione delle informazioni tra il team di AWS Security Incident Response e il cliente durante il processo di risposta all'incidente.

Contenimento, eliminazione e ripristino: prevenzione di ulteriori attività non autorizzate (contenimento), abbinata alla rimozione delle risorse non autorizzate e della vulnerabilità originaria (eradicazione), e recupero delle risorse per tornare alla normalità.

Miglioramento continuo: AWS Security Incident Response incorpora il feedback e le lezioni apprese dagli impegni precedenti per potenziarne le capacità di rilevamento, i processi investigativi e le azioni correttive. AWS Security Incident Response si attiene inoltre up-to-date alle più recenti minacce alla sicurezza e alle migliori pratiche per affrontare le sfide di sicurezza in continua evoluzione.

Evento di sicurezza informatica: un'azione che utilizza un sistema o una rete di informazioni per produrre un effetto negativo sul sistema, sulla rete o sulle informazioni in esso contenute.

Incidente di sicurezza informatica: violazione o minaccia imminente di violazione delle politiche di sicurezza informatica, delle politiche di utilizzo accettabile o delle pratiche di sicurezza standard.

Tecnici di Security Incident Response: un gruppo di individui che forniscono supporto durante eventi di sicurezza attivi. Per i casi AWS supportati, si tratta dei tecnici del Security Incident Response.

Flusso di lavoro di risposta agli incidenti: la sequenza definita di passaggi e attività coinvolti nella end-to-end gestione di un evento di sicurezza, in linea con lo standard NIST 800-61.

Strumenti investigativi: AWS Security Incident Response strumenti e ruoli collegati ai servizi utilizzati per esaminare lo stato operativo dell'account e delle risorse.

Lezioni apprese: la revisione e la documentazione della risposta a un evento di sicurezza per identificare le aree di miglioramento e informare la pianificazione della risposta agli incidenti futuri.

Monitoraggio e indagine: esamina AWS Security Incident Response rapidamente gli avvisi di sicurezza di Amazon GuardDuty, mettendo in primo piano gli avvisi più importanti che il tuo team deve analizzare. Configura le regole di soppressione in base alle specifiche dell'ambiente per prevenire avvisi non necessari.

Preparazione: le attività intraprese per preparare un'organizzazione a rispondere e gestire efficacemente gli eventi di sicurezza, come lo sviluppo di piani di risposta agli incidenti e procedure di test.

Segnalazione e comunicazione: i processi utilizzati per tenervi informati durante tutto il processo di risposta agli incidenti, tra cui notifiche automatiche, call bridge e consegna di elementi investigativi. AWS Security Incident Response fornisce un'unica dashboard centralizzata Console di gestione AWS per gestire tutti i tuoi sforzi. AWS Security Incident Response

Responder Generated Intelligence: indicatori di compromesso, tattiche, tecniche e procedure e modelli associati osservati dalle indagini. AWS

Competenza in materia di eventi di sicurezza: le conoscenze e le competenze specialistiche necessarie per rispondere e gestire efficacemente gli eventi di sicurezza, in particolare nel contesto del cloud. AWS

Modello di responsabilità condivisa: la divisione delle responsabilità di sicurezza tra il cliente AWS e il cliente, dove AWS è responsabile della sicurezza del cloud e il cliente è responsabile della sicurezza nel cloud.

Threat Intelligence: feed di dati interni ed esterni contenenti dettagli di attività non autorizzate per aiutare a identificare e rispondere alle minacce alla sicurezza in evoluzione.

Sistema di ticketing: una piattaforma dedicata alla gestione dei casi che consente di inserire e gestire casi di eventi di sicurezza, aggiungere allegati e monitorare il ciclo di vita della risposta agli incidenti.

Triage: la valutazione iniziale e l'assegnazione delle priorità di un evento di sicurezza per determinare la risposta appropriata e le fasi successive.

Flusso di lavoro: la sequenza definita di passaggi e attività coinvolti nella end-to-end gestione di un evento di sicurezza.

Nozioni di base

[Guida introduttiva con AWS Security Incident Response](#)

Indice

- [Guida all'onboarding](#)
- [Matrice RACI](#)
- [Seleziona un account di iscrizione](#)
- [Imposta i dettagli dell'iscrizione](#)
- [Associa gli account a AWS Organizations](#)
- [Imposta flussi di lavoro di risposta proattiva e valutazione degli avvisi](#)

Guida all'onboarding

La guida all'onboarding illustra i prerequisiti e le azioni di onboarding e AWS Security Incident Response contenimento.

Important

Prerequisiti

1. L'unico prerequisito per l'implementazione è l'abilitazione. [AWS Organizations](#)
2. Sebbene non sia obbligatorio, consigliamo di abilitare [Amazon GuardDuty](#) e [AWS Security Hub CSPM](#) su tutti gli account e di Regioni AWS attivarlo per massimizzare i vantaggi del Security Incident Response.
3. Revisione GuardDuty e risposta agli incidenti di sicurezza.
4. Consulta la [guida alle GuardDuty best practice](#).

AWS Security Hub CSPM raccoglie i risultati di fornitori terzi di endpoint detection and response (EDR) (Fortinet CrowdStrike (Lacework) e Trend Micro CrowdStrike, tra gli altri). Se questi risultati vengono inseriti in Security Hub CSPM, vengono valutati automaticamente da Security Incident Response per la creazione proattiva dei casi. Per configurare EDR di terze parti con Security Hub CSPM, consulta [Rileva](#) e analizza.

Per configurare EDR di terze parti con Security Hub CSPM:

1. Vai alla pagina Security Hub CSPM Integrazioni per verificare l'esistenza dell'integrazione di terze parti
2. Dalla console, vai alla pagina del servizio CSPM di Security Hub.
3. Scegli Integrazioni (usando Wiz.io come esempio):

The screenshot shows the AWS Security Hub CSPM console. The left sidebar is titled 'Security Hub CSPM' and includes a navigation menu with the following items: Summary (selected), Controls, Security standards, Insights, Findings, Integrations, Management (Automations, Custom actions), and Settings (General, Regions, Configuration, Usage). The main content area is titled 'Summary Info' and features a search bar and filter buttons for 'Workflow status' (NEW, NOTIFIED) and 'Record state' (ACTIVE). Below the filters, there is a section for 'Introducing the new AWS Security Hub - public preview' with a 'Try Security Hub' button. The 'Security standards' section shows a 'Security score' of 55% (288 of 524 controls passed) and a table of standards.

Standard	Passed	Failed	Score
CIS AWS Foundations Benchmark v3.0.0	13	23	35%
PCI DSS v3.1	--	--	---

4. Cerca il fornitore che desideri integrare

Integrations

Accept findings from other AWS services or from third-party integrations. You can also send findings from Security Hub CSPM to some integrations.



1 match



Wiz Security: Wiz Security

Description

Wiz continuously analyzes configurations, vulnerabilities, networks, IAM, secrets, and more across accounts, users, and workloads to discover the critical issues that represent the actual risk.

Type of integration

Sends findings to Security Hub CSPM

Categories

Cloud Security Posture Management, Third-Party Risk Assessment, Multi-Cloud Management

How to activate this integration

1. Purchase a subscription to this product: [Purchase](#)
2. Follow the integration's configuration instructions: [Configure](#)
3. Choose **Accept findings**

Status

Not accepting findings

[Accept findings](#)

Note

Quando richiesto, fornisci le informazioni sull'account o sull'abbonamento. Dopo aver fornito queste informazioni, Security Incident Response acquisisce i risultati di terze parti. Per esaminare i prezzi per l'acquisizione di risultati da terze parti, consulta la pagina Integrazioni in Security Hub CSPM.

Implementa e configura Security Incident Response

1. Scegli Registrati

Get started with AWS Security Incident Response

- Automatic monitoring and triaging of alerts
- Streamline security incident response
- Get 24/7 AWS security support and tools

[Sign up](#)

Pricing (USD)

Tier	Price per month
Tier 1 (First \$0 - \$125k)	\$7,000
Tier 2 (Next \$125k - \$250k)	5.00%
Tier 3 (Next \$250k - \$500k)	3.50%
Tier 4 (Next \$500k - \$1M)	1.50%
Tier 5 (>\$1M)	0.50%

[Learn more](#)

2. Seleziona un account per gli strumenti di sicurezza come amministratore delegato dall'account di gestione.

- [Architettura di riferimento per la sicurezza](#)
- [Documentazione per amministratori delegati](#)

Set up central membership account

▼ What is the purpose of the central membership account?

Centralized account location
Create, manage, and access active and resolved security cases.

Manage membership
Modify and change membership configurations including permissions, contacts, and more.

Central membership account
It is recommended that you align your AWS Security Incident Response central account to the same administrator account you have enabled for services such as Amazon GuardDuty and AWS Security Hub.

Use delegated administrator account - Recommended
Delegated administrator account can manage membership and cases.

Use this account
Use this account to manage membership and cases.

Delegated administrator

Account ID
Must be 12 digits. Must be in your AWS Organizations.

SECURITY-TOOLING-ACCOUNT-NUMBER

Account ID must be 12 digits

[Delegate](#)

3. Accedi all'account amministratore delegato

4. Inserisci i dettagli dell'iscrizione e gli account associati

The screenshot shows the 'Define membership details' step of the AWS Security Incident Response onboarding process. A vertical sidebar on the left lists five steps: Step 1 (Set up central membership account), Step 2 (Define membership details - selected), Step 3 (Permissions for proactive response), Step 4 (Review service permissions), and Step 5 (Review and sign up). The main content area is titled 'Define membership details' and contains four sections:

- Membership region**: A section with a description and a 'Region selection' dropdown menu currently set to 'US East (N. Virginia)'.
- Associate accounts**: A section with a description and two radio button options: 'Associate entire AWS Organization' (selected) and 'Associate part of your AWS Organization'.
- Membership name**: A section with a description and a text input field containing 'Demo Security Incident Response'.
- Membership contacts**: A section with a description and a 'Primary contact' form with three input fields: 'Name' (Kyle Shields), 'Job title' (SOC Commander), and 'Email' (ks@amazon.com).

Autorizza le azioni di Security Incident Response

Questa pagina descrive come autorizzare Security Incident Response a eseguire azioni automatiche di monitoraggio e contenimento nell'ambiente. AWS È possibile abilitare due funzioni di autorizzazione distinte: il monitoraggio proattivo della risposta e le preferenze relative alle azioni di contenimento. Queste funzionalità sono indipendenti e possono essere abilitate separatamente in base ai requisiti di sicurezza.

Abilita Proactive Response

La risposta proattiva consente a Security Incident Response di monitorare e analizzare gli avvisi generati da Amazon GuardDuty e AWS Security Hub CSPM le integrazioni all'interno dell'organizzazione. Se abilitata, Security Incident Response classifica gli avvisi a bassa priorità con l'automazione dei servizi in modo che il team possa concentrarsi sui problemi più critici.

Per abilitare una risposta proattiva durante l'onboarding:

1. Nella console Security Incident Response, accedi al flusso di lavoro di onboarding.

- Rivedi le autorizzazioni di servizio che consentono a Security Incident Response di monitorare i risultati di tutti gli account coperti e attivi supportati Regioni AWS nella tua organizzazione.
- Scegli Iscriviti per abilitare la funzionalità.

Step 1 Set up central membership account

Step 2 Define membership details

Step 3 Permissions for proactive response

Step 4 **Review service permissions**

Step 5 Review and sign up

Review service permissions

Enable Security Incident Response
The following permissions are enabled by default when you sign up for AWS Security Incident Response.

By setting up AWS Security Incident Response, expect the following:

- Service-linked roles:** AWS Security Incident Response will have the necessary permissions to access all of the organizational units (OUs) and their accounts within your AWS Organizations infrastructure to create the service membership.
 - [View permission details](#)
- Log Access and Investigation:** In order to expedite response and recovery, you are granting AWS Security Incident Response the ability to work with internal AWS teams to access and review logs for incident investigation and response. These include analyzing log sources such as Amazon VPC Flow Logs, AWS CloudTrail management events, and Amazon S3 CloudTrail events.

Configuration settings for data sources
Security Incident Response does not manage the data, events, and logs for your AWS accounts and environments. You can manage these data sources through the respective AWS services consoles or APIs.

Step 1 Set up central membership account

Step 2 Define membership details

Step 3 Permissions for proactive response

Step 4 Review service permissions

Step 5 **Review and sign up**

Review and sign up

Step 1: Set up central membership account [Edit](#)

Central membership account

Account type: Delegated administrator
Use delegated administrator account

Step 2: Define membership details [Edit](#)

Membership details

Region: US East (N. Virginia) | Name: Demo Security Incident Response

Associated accounts

Accounts: Associate entire AWS Organization

Membership contacts

Name	Job title	Email
Matt Meck	Incident Response Lead	mm@amazon.com
Kyle Shields	SOC Commander	ks@amazon.com

Membership tags

Key | Value

No tags

Questa funzione crea automaticamente un ruolo collegato al servizio in tutti gli account membro coperti all'interno del tuo. AWS Organizations Tuttavia, è necessario creare manualmente il ruolo collegato al servizio nell'account di gestione utilizzando i set di stack. AWS CloudFormation

Passaggi successivi: per ulteriori informazioni su come funziona Security Incident Response con Amazon GuardDuty AWS Security Hub CSPM, consulta Detect and Analyze nella Guida per l'AWS Security Incident Response utente.

Definisci le preferenze relative alle azioni di contenimento

Le azioni di contenimento consentono AWS Security Incident Response di eseguire misure di risposta rapida durante un incidente di sicurezza attivo. Queste azioni aiutano a mitigare rapidamente l'impatto degli incidenti di sicurezza nell'ambiente.

Important

Security Incident Response non abilita le funzionalità di contenimento per impostazione predefinita. È necessario autorizzare esplicitamente le azioni di contenimento tramite le preferenze di contenimento.

Per autorizzare i AWS Security Incident Response tecnici a eseguire azioni di contenimento per tuo conto, oltre a implementare un programma [AWS CloudFormation StackSet](#) che crei i ruoli IAM richiesti, devi definire le preferenze di contenimento a livello di organizzazione o account. Le preferenze a livello di account sostituiscono le preferenze a livello di organizzazione.

Prerequisiti: è necessario disporre delle autorizzazioni per creare casi. Supporto AWS

Opzioni di contenimento:

- Approvazione richiesta (impostazione predefinita): non eseguire il contenimento proattivo di alcuna risorsa senza un'autorizzazione esplicita su base regolare. case-by-case
- Contenimento confermato: esegui il contenimento proattivo di una risorsa confermata compromessa.
- Contenimento dei dati sospetti: esegui il contenimento proattivo di una risorsa con un'alta probabilità che sia stata compromessa, sulla base di un'analisi eseguita dai tecnici. AWS Security Incident Response

Per definire le preferenze di contenimento:

1. [Crea un Supporto AWS caso](#) per richiedere la configurazione delle preferenze relative alle azioni di contenimento per Security Incident Response.
2. Nel caso di assistenza, specifica:
 - Il tuo AWS Organizations ID o l'account specifico IDs in cui devono essere autorizzate le azioni di contenimento

- L'opzione di contenimento preferita (è richiesta l'approvazione, il contenuto è confermato o il contenuto sospetto).
 - I tipi di azioni di contenimento che desideri autorizzare (come l'isolamento delle istanze EC2, la rotazione delle credenziali o le modifiche ai gruppi di sicurezza)
3. Supporto AWS collabora con te per configurare le tue preferenze di contenimento. È necessario implementare il necessario per creare AWS CloudFormation StackSet i ruoli IAM richiesti. Supporto AWS può fornire assistenza, se necessario.

Una volta configurato, AWS Security Incident Response esegue le azioni di contenimento autorizzate durante gli incidenti di sicurezza attivi per contribuire a proteggere l'ambiente.

Passaggi successivi: dopo aver configurato le preferenze di contenimento, è possibile monitorare le azioni di contenimento intraprese durante gli incidenti nella console Security Incident Response.

Dopo l'implementazione di Security Incident Response

AWS si integra con il framework di risposta agli incidenti esistente anziché sostituirlo.

1. Esamina le nostre capacità di integrazione operativa per migliorare le tue pratiche attuali.
2. Guarda la nostra demo di supporto, EventBridge utilizzo e integrazione Jira-ITSM per operazioni di sicurezza più efficienti per i soci a livello di UO.

[AWS Security Incident Response: Nuove integrazioni e abbonamento a livello di OU](#)

Aggiorna l'Incident Response Team

1. Assicurati di essere abbonato e di aver completato i passaggi di onboarding descritti in questa guida di onboarding.
2. Seleziona Incident Response Team dalla barra di navigazione a sinistra.
3. Seleziona i compagni di squadra che desideri aggiungere al tuo team.

Incident Response Team info

► Set up your Incident Response Team

Teammates (10/10) Edit Delete Add

You can specify up to 10 members in your Incident Response Team. Additional members can be added for individual cases.

<input type="checkbox"/>	Name	▲ Job title	▼ Email
<input type="checkbox"/>	Brian Boyd	Network Analyst Lead	brianb@anycompany.com
<input type="checkbox"/>	Chris Beck	Blue Team Lead	chrisb@anycompany.com
<input type="checkbox"/>	David Buckendorf	Incident Response Manager	davidb@anycompany.com
<input type="checkbox"/>	John Bheuler	SOC Commander	johnb@anycompany.com
<input type="checkbox"/>	Jordan Schroff	SOC Operations Manager	jordans@anycompany.com
<input type="checkbox"/>	Kyle Prime	Detection Lead	wearekyle@anycompany.com

Note

Il team può includere dirigenti dell'organizzazione, consulenti legali, partner MDR, ingegneri del cloud e altri. Puoi aggiungere fino a 10 membri aggiuntivi. Includi solo nome, titolo e indirizzo email per ogni membro.

AWS caso supportato

AWS Security Incident Response fornisce un portale di gestione dei casi basato su abbonamento in cui l'organizzazione interagisce direttamente con i nostri tecnici di Security Incident Response. Forniamo assistenza nelle indagini di sicurezza e negli incidenti attivi con un SLO di 15 minuti, senza limiti di casi reattivi. Consulta la nostra documentazione relativa alla creazione di un AWS caso supportato.

Espandi il team investigativo

Tramite il Case Management Portal, puoi garantire la visibilità dei casi a parti esterne aggiungendo Watchers e policy IAM. Utilizza queste opzioni per partner, team legali o esperti in materia.

Per aggiungere Watchers a un caso:

1. Apri qualsiasi caso dal portale Security Incident Response Cases.

Cases (19) Create case

ID	Last updated	Resolver	Title	Type	Status	Created at
7375520993	23 hours ago	Self	CIRT - Proactive Case - Possible threat actor on a malicious Known Domain	Security Incident	Submitted	3 days ago
0512611769	5 days ago	Self	Jira Test Case - SHOWCASE INTEGRATION - On-Going	Security Incident	Submitted	2 months ago
5191116623	2 months ago	Self	Active Incident [2025-7-15] Test Case - Jira	Security Incident	Closed	2 months ago
0928191969	2 months ago	Self	CIRT - Proactive Case - Customer Servers Compromised (CrowdStrike Finding)	Security Incident	Detection & Analysis	2 months ago
9545275838	2 months ago	Self	Active Incident [2025-7-14] - Integration Test with Jira	Security Incident	Closed	2 months ago
7729907189	2 months ago	Self	Active Incident [2025-7-14] - TEST EVENTBRIDGE INTEGRATION WITH SNS JIRA	Security Incident	Closed	2 months ago
8052835544	2 months ago	Self	Active Incident [2025-7-14] - TEST TO EVENTBRIDGE INTEGRATION	Security Incident	Closed	2 months ago
6026939273	2 months ago	Self	CIRT - Reactive Case - Customer Website Compromised	Security Incident	Post-incident activities	2 months ago
1483356434	2 months ago	Self	CIRT - Proactive Case - Customer Access Keys compromised	Security Incident	Post-incident activities	2 months ago

2. Scegli la scheda Autorizzazioni

0928191969 Edit Actions Get help from AWS

Overview

Resolver
Self

Name
CIRT - Proactive Case - Customer Servers Compromised (CrowdStrike Finding)

Type
Security Incident

arn
arn:aws:security-irus-east-1:854725306385:cas:e/0928191969

Created at
2025-07-14T11:08:03-07:00

Start date estimate
2025-07-15

Incident start date (actual)
-

Status
Detection & Analysis

Actions
-

Last updated
2 months ago

Details | Communications | **Permissions** | Attachments | Tags | Case activities

Watchers (3/30) Remove Add

Watchers will receive notifications related to this case. All members of your Incident Response Team will also receive these notifications.

Search

Name	Job title	Email
<input type="checkbox"/> Jon "Application" Doe	Lead Application Architect	applicationSME@anycompany.com
<input type="checkbox"/> Legal Team	Corporate Lawyer	legalteam@anycompany.com
<input type="checkbox"/> Our MSSP Vendor	MSSP Vendor	msspVendor@mssp.com

Incident response team (10) Go to Incident Response Team

All members of your Incident Response Team will also receive notifications for this case.

3. Seleziona Aggiungi

Details | Communications | **Permissions** | Attachments | Tags | Case activities

Watchers (3/30) Remove Add

Watchers will receive notifications related to this case. All members of your Incident Response Team will also receive these notifications.

Search

Name	Job title	Email
<input type="checkbox"/> Jon "Application" Doe	Lead Application Architect	applicationSME@anycompany.com
<input type="checkbox"/> Legal Team	Corporate Lawyer	legalteam@anycompany.com
<input type="checkbox"/> Our MSSP Vendor	MSSP Vendor	msspVendor@mssp.com

Incident response team (10) Go to Incident Response Team

All members of your Incident Response Team will also receive notifications for this case.

Template case permission policy Go to IAM Copy to clipboard

Use this sample policy in IAM to define permissions for this case.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SecurityIncidentResponseCaseReadAccess",
      "Effect": "Allow",
      "Action": [
        "security-irus:GetCase",
        "security-irus:GetCaseAttachmentDownloadUrl",
        "security-irus:ListComments",
        "security-irus:ListCaseEdits",
        "security-irus:ListTagsForResource"
      ]
    }
  ]
}
    
```

Note

Ogni caso include una policy IAM precompilata che garantisce l'accesso solo a quel caso specifico, mantenendo il privilegio minimo. Copia e incolla questa policy direttamente nei ruoli o negli utenti IAM per consentire il loro contributo a partner MDR di terze parti o team investigativi specifici.

GuardDuty risultati e regole di soppressione

AWS Security Incident Response acquisisce, valuta e risponde in modo proattivo a tutti i risultati di Amazon e ai GuardDuty risultati di FortinetTCNApp (CrowdStrikeLacework) e AWS Security Hub CSPM Trend Micro. La nostra tecnologia di valutazione automatica elimina i requisiti di analisi interna. Il servizio crea regole di soppressione e archiviazione automatica in GuardDuty Security Hub CSPM per risultati benigni. Visualizza o modifica queste regole in «Findings» nella GuardDuty console Amazon.

Per rivedere le regole di GuardDuty soppressione abilitate, completa i seguenti passaggi:

1. Apri la GuardDuty console Amazon.
2. Scegli Findings.
3. Nel riquadro di navigazione, scegli Regole di soppressione. La pagina Regole di soppressione mostra un elenco di tutte le regole di soppressione per il tuo account.
4. Per rivedere o modificare le impostazioni di una regola, scegli la regola, quindi scegli Aggiorna regola di soppressione dal menu Azioni.

Note

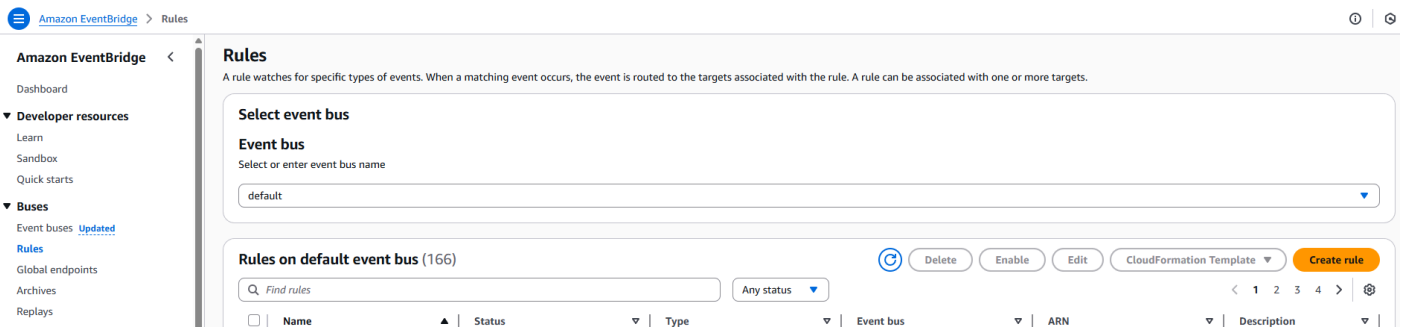
Le organizzazioni che utilizzano la tecnologia SIEM hanno ridotto significativamente i volumi di GuardDuty ricerca nel tempo, migliorando sia il servizio Security Incident Response che l'efficienza SIEM.

Amazon EventBridge

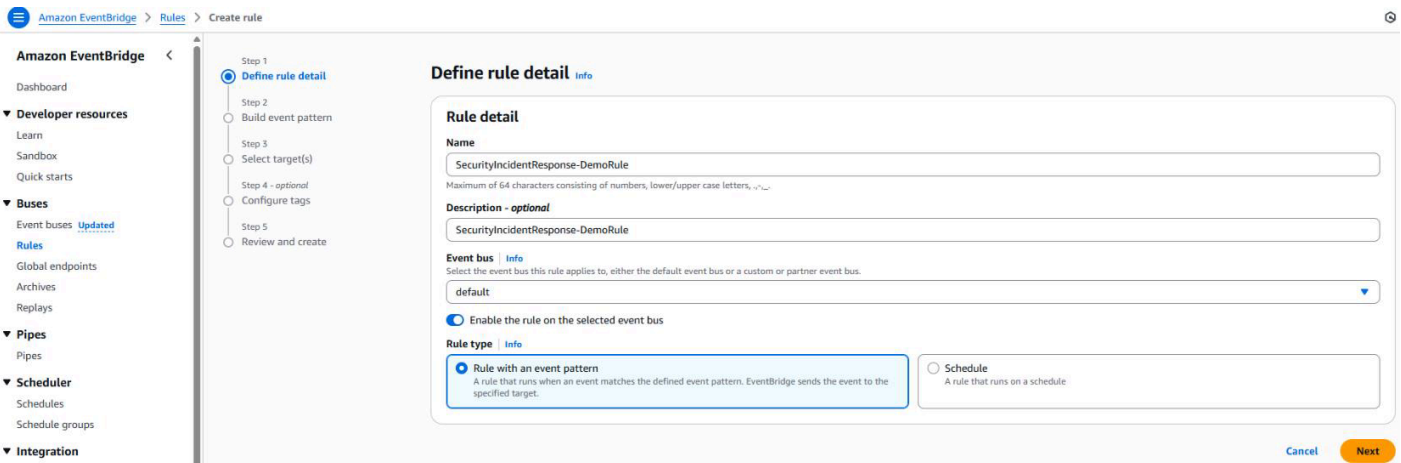
Amazon EventBridge abilita un'architettura basata sugli eventi per Security Incident Response, che consente all'attività dei casi di attivare servizi downstream (SNS, Lambda, SQS, Step-Functions) o strumenti esterni (Jira, Teams, Slack,). ServiceNow PagerDuty

EventBridge Per configurare le regole:

1. Accedi ad Amazon EventBridge
2. Seleziona Regole dal menu a discesa Autobus.



3. Selezionare Create Rule (Crea regola).
4. Inserisci i dettagli della regola.
5. Scegli Next (Successivo).



6. Scorri fino a AWS service, quindi seleziona AWS Security Incident Response dal menu a discesa.

Event pattern [Info](#)

Creation method

Use schema
Use an Amazon EventBridge schema to generate the event pattern.

Use pattern form
Use a template provided by EventBridge to create an event pattern.

Custom pattern (JSON editor)
Write an event pattern in JSON.

Q security

- Amazon Security Lake
- AWS Security Incident Response
- Security Hub
- Security Token Service (STS)

Select a service provider

Event pattern
Event pattern, or filter to match the events

```
1
```

- Dal menu a discesa Tipo di evento, seleziona l'evento o la chiamata API per cui desideri creare un pattern.
- Puoi modificare manualmente il modello per includere più di un evento.
- Scegli Next (Successivo).

Event pattern [Info](#)

Creation method

Use schema
Use an Amazon EventBridge schema to generate the event pattern.

Use pattern form
Use a template provided by EventBridge to create an event pattern.

Custom pattern (JSON editor)
Write an event pattern in JSON.

Event source
AWS service or EventBridge partner as source

AWS services

AWS service
The name of the AWS service as the event source

AWS Security Incident Response

Event type
The type of events as the source of the matching pattern

Case Created

Event pattern
Event pattern, or filter to match the events

```
1 {
2   "source": ["aws.security-ir"],
3   "detail-type": ["case created"]
4 }
```

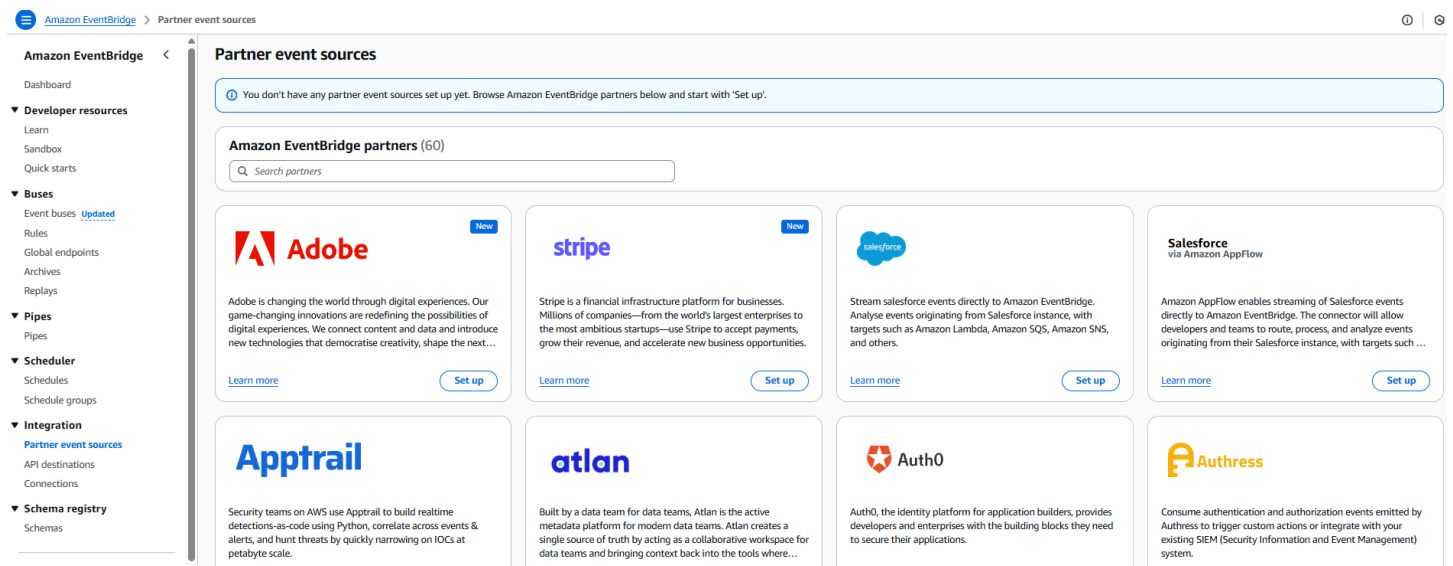
Copy Test pattern Edit pattern

Cancel Previous Next

Note

Seleziona uno o più obiettivi (Amazon Simple Notification Service AWS Lambda, documento SSM, Step-Function) per i tuoi eventi. Se necessario, configura obiettivi per più account.

Puoi verificare i modelli di integrazione dei partner in Partner Event Sources nel menu EventBridge Integrazione. I partner disponibili includono Atlassian (Jira), New Relic DataDog, Symantec e PagerDuty Zendesk, tra molti altri.



Integrazioni e flusso di lavoro con strumenti esterni

AWS soluzioni per integrare JIRA o ServiceNow con Security Incident Response

Implementa le nostre soluzioni completamente sviluppate per l'integrazione bidirezionale con Jira e ServiceNow. Queste integrazioni consentono la comunicazione bidirezionale tra AWS Security Incident Response Cases e la tua piattaforma ITSM, con gli aggiornamenti dei casi riflessi automaticamente nelle attività Jira corrispondenti.

Vantaggi dell'integrazione

L'integrazione AWS Security Incident Response con la piattaforma ITSM esistente semplifica le operazioni di sicurezza centralizzando i flussi di lavoro di tracciamento e risposta agli incidenti. Queste soluzioni predefinite eliminano la necessità di uno sviluppo personalizzato, consentendo ai team di sicurezza di mantenere la visibilità sui sistemi di gestione degli incidenti sia AWS nativi che a livello aziendale. Sfruttando Amazon EventBridge per l'automazione basata sugli eventi, gli aggiornamenti fluiscono senza interruzioni tra le piattaforme in tempo reale, contribuendo a garantire che gli incidenti di sicurezza vengano tracciati in modo coerente indipendentemente dalla loro origine. Questo approccio unificato riduce il cambio di contesto per gli analisti della sicurezza, migliora i tempi di risposta e fornisce audit trail completi per l'intero ciclo di vita della risposta agli incidenti.

Per configurare le regole: EventBridge

1. Accedi ad Amazon EventBridge.
2. Seleziona Regole dal menu a discesa Autobus.

Flusso di lavoro con utensili esterni

Security Incident Response si integra con strumenti e partner esterni in diversi modi:

- **Integrazione SIEM:** gli ingegneri di Security Incident Response aiutano ad analizzare e indagare su tali risultati in parallelo con il tuo team quando invii i casi AWS supportati. Identifichiamo le correlazioni tra ambienti ibridi e multi-cloud, aiutando a monitorare i movimenti degli autori delle minacce tra i provider.
- **Migliora le tue operazioni di sicurezza esistenti:** sostituiamo i flussi di lavoro di GuardDuty risposta tradizionali con un modello di risposta parallelo più efficiente. Molte organizzazioni attualmente utilizzano la tecnologia SIEM per i flussi di lavoro di rilevamento attraverso la gestione dei casi. Questo servizio offre un'alternativa semplificata, specifica per GuardDuty (e per alcuni selezionati Security Hub CSPM). La soluzione sfrutta una sofisticata tecnologia di valutazione automatica con supervisione umana per creare casi proattivi nel portale, avvisando contemporaneamente il team di risposta e coinvolgendo i nostri tecnici di Security Incident Response per interventi correttivi coordinati.
- **Team investigativi di terze parti:** i nostri tecnici di Security Incident Response collaborano direttamente con i vostri partner e i fornitori di MDR.

Appendice A: Punti di contatto

Fornire i metadati in anticipo ai nostri tecnici di Security Incident Response può contribuire ad accelerare i tempi di creazione del profilo, aumentando la fiducia nella nostra tecnologia di triaging fin dall'inizio. Questo aiuta a ridurre i falsi positivi iniziali identificati quando iniziamo ad assimilare le scoperte sulle minacce e a creare il «mondo buono conosciuto».

Informazioni di contatto del personale IR e SOC

Voc	Persona IR SOC: ruolo, nome, email	Contatti primari e secondari	Interventi interni e noti	Interventi esternali e noti	Fornitori di servizi cloud aggiuntivi	AWS Regioni di lavoro	Server DNS IPs (se diversi da Amazon Route 53 Resol	VPN Soluzioni di accesso remoto e IPs	Nomi di applicazioni critiche Numeri di account	Porte non comuni utilizzate	EDR AV Strumenti di gestione delle vulnerabilità utilizzati	IDP Sedi
1	Comandante del SOC, John Smith, jsmith@ample.c	Prima	10.0.0.16	5.5.60.20 (Azzu	Azure	us-east-1, us-east-2	N/D	Direct Connect VIF pubblica 116.32.87	Server Web Nginx (esempi critico) 12345670	8080	CrowdStrike Falco	Entra, Azure

[Per inviare informazioni sui metadati per il tuo ambiente, crea un Supporto AWS caso.](#)

Per inviare i metadati

1. Completa la tabella dei metadati con le informazioni sull'ambiente.
2. Crea un Supporto AWS caso con i seguenti dettagli:
 - Tipo di custodia: tecnica
 - Servizio: Servizio di risposta agli incidenti di sicurezza
 - Categoria: Altro

3. Allega la tabella di metadati completata al case.

Matrice RACI

La seguente matrice RACI definisce i ruoli e le responsabilità nell'ambito del processo di implementazione del Security Incident Response. RACI sta per Responsabile (R), Accountable (A), Consulted (C) e Informed (I).

Attività	Cliente	AWS Team addetto all'account	Squadra SIR
Preimbarco			
Identifica i principali stakeholder	R		I
Convalida le fonti di ricerca	R	C	I
[Integrazione EDR di terze parti] Security Hub CSPM	R	C	I
GuardDuty Convalida/controllo dello stato	C	R	I
Determina l'ambito dell'account	R		
Stabilisci protocolli di escalation	R	I	C
Abilita AWS Organizzazioni	R	C	
Associa gli account a AWS Organizzazioni	R	I	
Seleziona Amministratore delegato/ Account di sicurezza	R	I	
Onboarding			
Imposta i dettagli dell'iscrizione	R	I	

Attività	Cliente	AWS Team addetto all'account	Squadra SIR
Procedura dettagliata (impostazione dei flussi di lavoro di risposta proattiva e classificazione degli avvisi; distribuzione del ruolo collegato al servizio nell'account di gestione; autorizzazione delle azioni di contenimento)	R	C	I
Configurazione post-implementazione			
Esamina le capacità di integrazione operativa	R	C	I
Invia casi reattivi di risposta agli incidenti di sicurezza	R		
Configura le EventBridge integrazioni Amazon	R	C	C
Connect strumenti di terze parti (Jira,, ServiceNow PagerDuty, Teams, ecc.)	R	I	C
Approfondimento del servizio e demo	A	R	C

Definizioni RACI:

- Responsabile (R) - La parte che esegue il lavoro per completare l'attività
- Responsabile (A): la parte in ultima analisi responsabile del corretto completamento dell'attività
- Consultato (C) - La parte di cui vengono richieste le opinioni e con la quale esiste una comunicazione bidirezionale
- Informata (I) - La parte che viene mantenuta up-to-date sui progressi e con la quale esiste una comunicazione unidirezionale

Seleziona un account di iscrizione

Un account di iscrizione è l' AWS account utilizzato per configurare i dettagli dell'account, aggiungere e rimuovere dettagli per il team di risposta agli incidenti e dove è possibile creare e gestire tutti gli eventi di sicurezza attivi e storici. Ti consigliamo di allineare il tuo account di AWS Security Incident Response iscrizione allo stesso account che hai abilitato per servizi come Amazon GuardDuty e AWS Security Hub CSPM.

Hai due opzioni per selezionare il tuo account di AWS Security Incident Response iscrizione utilizzando AWS Organizations. È possibile creare un'iscrizione nell'account di gestione Organizations o in un account amministratore delegato di Organizations.

Utilizza l'account amministratore delegato: le attività AWS Security Incident Response amministrative e la gestione dei casi si trovano nell'account amministratore delegato. Ti consigliamo di utilizzare lo stesso amministratore delegato che hai impostato per altri servizi di AWS sicurezza e conformità. Fornisci l'ID dell'account amministratore delegato a 12 cifre, quindi accedi a tale account per procedere.

Important

Quando utilizzi un account amministratore delegato come parte della configurazione, non AWS Security Incident Response puoi creare automaticamente il ruolo collegato al servizio di triage richiesto nell'account di gestione. AWS Organizations
Puoi utilizzare IAM per creare questo ruolo nel tuo AWS Organizations account di gestione

Come creare un ruolo collegato ai servizi (console)

1. Accedi al tuo account AWS Organizations di gestione.
2. Accedi alla [AWS CloudShell](#) finestra o accedi all'account tramite CLI nel tuo metodo preferito.
3. Usa il comando CLI `aws iam create-service-linked-role --aws-service-name "triage.security-ir.amazonaws.com" --no-cli-pager`
4. (Facoltativo) Per verificare che il comando abbia funzionato, puoi eseguirlo `aws iam get-role --role-name AWSServiceRoleForSecurityIncidentResponse_Triage`

Usa l'account attualmente connesso: selezionando questo account, l'account corrente verrà designato come account di iscrizione centrale per la tua AWS Security Incident Response iscrizione. Le persone all'interno dell'organizzazione dovranno accedere al servizio tramite questo account per creare, accedere e gestire i casi attivi e risolti.

Assicurati di disporre di autorizzazioni sufficienti per l'amministrazione AWS Security Incident Response.

Fai riferimento a [Aggiungere e rimuovere le autorizzazioni di identità IAM per i passaggi specifici per aggiungere le autorizzazioni](#).

Fai riferimento alle politiche [AWS Security Incident Response gestite](#).

Per verificare le autorizzazioni IAM, puoi seguire questi passaggi:

- Verifica la politica IAM: esamina la policy IAM allegata al tuo utente, gruppo o ruolo per assicurarti che conceda le autorizzazioni necessarie. Puoi farlo accedendo a <https://console.aws.amazon.com/iam/>, selezionando l'Users opzione, scegliendo l'utente specifico e quindi nella pagina di riepilogo, vai alla Permissions scheda in cui puoi vedere un elenco di tutte le politiche allegate; puoi espandere ogni riga della policy per visualizzarne i dettagli.
- Verifica le autorizzazioni: prova a eseguire l'azione necessaria per verificare le autorizzazioni. Ad esempio, se devi accedere a un caso, prova a farlo. ListCases Se non disponi delle autorizzazioni necessarie, riceverai un messaggio di errore.
- Usa il AWS CLI o SDK: puoi utilizzare AWS Command Line Interface o un AWS SDK nel tuo linguaggio di programmazione preferito per testare le autorizzazioni. Ad esempio, con AWS Command Line Interface, puoi eseguire il `aws sts get-caller-identity` comando per verificare le autorizzazioni utente correnti.
- Controlla AWS CloudTrail i log: [esamina i CloudTrail log](#) per vedere se le azioni che stai tentando di eseguire vengono registrate. Questo può aiutarti a identificare eventuali problemi di autorizzazione.
- Usa il simulatore di policy IAM: [il simulatore di policy IAM](#) è uno strumento che ti consente di testare le policy IAM e vedere l'effetto che hanno sulle tue autorizzazioni.

Note

I passaggi specifici possono variare a seconda del AWS servizio e delle azioni che stai cercando di eseguire.

Imposta i dettagli dell'iscrizione

- Seleziona un Regione AWS luogo in cui archiviare l'iscrizione e i casi.

Warning

Non puoi modificare l'impostazione predefinita Regione AWS dopo la registrazione iniziale dell'iscrizione.

- Seleziona se desideri fornire una copertura associativa completa AWS Organizations o parziale a tutte AWS Organizations le unità organizzative (OUs).
- Facoltativamente, puoi selezionare un nome per questo abbonamento.
- È necessario fornire un contatto principale e uno secondario come parte del flusso di lavoro per la creazione dell'iscrizione. Questi contatti vengono automaticamente inclusi come parte del team di risposta agli incidenti. Per ogni iscrizione devono esistere almeno due contatti, il che garantisce inoltre l'inclusione di almeno due contatti nel team di risposta agli incidenti.
- Definisci tag opzionali per la tua iscrizione. I tag ti aiutano a tenere traccia AWS dei costi e a cercare risorse.

Associa gli account a AWS Organizations

Se hai scelto di associare tutti i tuoi account AWS Organizations durante la configurazione, l'iscrizione dà diritto alla copertura di tutti gli account dei membri dell'organizzazione. Gli account associati verranno aggiornati automaticamente non appena gli account vengono aggiunti o rimossi dall'organizzazione.

Se hai scelto di associare parte del tuo account AWS Organizations durante la configurazione e hai limitato l'iscrizione a unità organizzative specifiche (OUs), l'iscrizione dà diritto alla copertura di tutti gli account compresi tra quelli selezionati OUs. Sono inclusi gli account inferiori a quelli OUs selezionati. OUs Gli account associati si aggiornano automaticamente non appena gli account vengono aggiunti o rimossi da tali OUs account.

Per ulteriori informazioni sulle best practice relative alle unità organizzative, consulta [Organizzare AWS l'ambiente utilizzando più account](#).

Imposta flussi di lavoro di risposta proattiva e valutazione degli avvisi

AWS Security Incident Response monitora e analizza gli avvisi di minaccia generati dalle integrazioni CSPM di Amazon e Security GuardDuty Hub. Per utilizzare questa funzionalità, [Amazon GuardDuty deve essere abilitato](#). AWS Security Incident Response classifica gli avvisi a bassa priorità con l'automazione dei servizi in modo che il team possa concentrarsi sui problemi più critici. Per ulteriori informazioni su come AWS Security Incident Response funziona con Amazon GuardDuty and AWS Security Hub CSPM, consulta la sezione [Rileva e analizza](#) della guida per l'utente.

Se riscontri problemi di onboarding, [crea un Supporto AWS caso per richiedere](#) ulteriore assistenza. Assicurati di includere i dettagli, tra cui l' Account AWS ID e gli eventuali errori che potresti aver riscontrato durante il processo di configurazione.

Note

Se hai domande sulle regole di GuardDuty soppressione di Amazon, sulle configurazioni di classificazione degli avvisi o sui flussi di lavoro di risposta proattiva, puoi creare un caso AWS supportato con il tipo di caso Investigations and Inquiries e consultare il team di Security Incident Response. AWS Per ulteriori informazioni, consulta [Crea un caso AWS supportato](#).

Questa funzionalità consente di monitorare e analizzare AWS Security Incident Response i risultati in tutti gli account coperti e nelle regioni supportate attive della tua organizzazione. AWS Per facilitare questa funzionalità, crea AWS Security Incident Response automaticamente un ruolo collegato al servizio in tutti gli account dei soci coperti all'interno dell'azienda. AWS Organizations Tuttavia, per l'account di gestione, è necessario creare manualmente il ruolo collegato al servizio per abilitare il monitoraggio.

Il servizio non può creare il ruolo collegato al servizio nell'account di gestione. È necessario creare questo ruolo manualmente nell'account di gestione utilizzando i set [di AWS CloudFormation stack](#).

Comprendere l'archiviazione automatica con Proactive Response

Quando abiliti la risposta proattiva e il triaging degli avvisi, monitora e AWS Security Incident Response classifica automaticamente i risultati di sicurezza di Amazon e Security GuardDuty Hub CSPM. Nell'ambito di questo flusso di lavoro di valutazione automatica, i risultati vengono archiviati automaticamente in base ai seguenti criteri:

Comportamento di archiviazione automatica:

- **Risultati innocui:** quando il processo di valutazione automatica determina che un risultato è benigno (non una vera minaccia alla sicurezza), archivia AWS Security Incident Response automaticamente il risultato in Amazon GuardDuty e crea regole di soppressione per evitare che risultati simili generino avvisi in futuro.
- **Regole di soppressione:** il servizio crea regole di soppressione e archiviazione automatica sia in Amazon che in Security GuardDuty Hub CSPM per risultati che corrispondono ai modelli noti e validi del tuo ambiente, come gli indirizzi IP previsti, le entità IAM e i normali comportamenti operativi.
- **Volume di avvisi ridotto:** le organizzazioni che utilizzano la tecnologia SIEM registrano una significativa riduzione dei volumi di GuardDuty ricerca di Amazon nel tempo, man mano che il servizio apprende il tuo ambiente e archivia automaticamente i risultati benigni. Ciò migliora l'efficienza sia del AWS Security Incident Response servizio che del SIEM.

Visualizzazione dei risultati archiviati:

È possibile esaminare automaticamente i risultati archiviati e le regole di soppressione create da: AWS Security Incident Response

1. Passa alla GuardDuty console Amazon
2. Scegli Findings
3. Seleziona Archiviato dal filtro dei risultati
4. Rivedi le regole di soppressione selezionando la freccia rivolta verso il basso accanto a ciascuna regola

Considerazioni importanti:

- I risultati archiviati vengono conservati in Amazon GuardDuty per 90 giorni e possono essere visualizzati in qualsiasi momento durante tale periodo.
- Puoi modificare o eliminare le regole di soppressione in qualsiasi momento tramite la console Amazon GuardDuty
- Il processo di valutazione automatica si adatta continuamente all'ambiente, migliorando la precisione nel tempo e riducendo i falsi positivi

Contenimento: in caso di incidente di sicurezza, AWS Security Incident Response può eseguire azioni di contenimento per mitigare rapidamente l'impatto, come isolare gli host compromessi o ruotare le credenziali. Security Incident Response non abilita le funzionalità di contenimento per impostazione predefinita. Per eseguire queste azioni di contenimento, è necessario innanzitutto concedere le autorizzazioni necessarie al servizio. Ciò può essere fatto implementando un [AWS CloudFormation StackSet](#), che crea i ruoli richiesti.

Attività dell'utente

Indice

- [Pannello di controllo](#)
- [Gestire il mio Incident Response Team](#)

Pannello di controllo

Sulla AWS Security Incident Response console, la dashboard offre una panoramica del team di risposta agli incidenti, dello stato di risposta proattiva e un conteggio progressivo dei casi per quattro settimane.

Team di risposta agli incidenti

Seleziona Visualizza il team di risposta agli incidenti per accedere ai dettagli dei tuoi colleghi del team di risposta agli incidenti.

I miei casi

La sezione I miei casi della dashboard mostra il numero di casi AWS supportati aperti e chiusi, oltre ai casi autogestiti assegnati all'utente entro un periodo definito. Mostra anche il tempo medio impiegato per risolvere i casi chiusi, espresso in ore.

Gestire il mio Incident Response Team

I tuoi team di risposta agli incidenti contengono le parti interessate al processo di risposta agli incidenti. Puoi configurare fino a dieci parti interessate come parte della tua iscrizione.

Gli esempi per le parti interessate interne includono i membri del team di risposta agli incidenti, gli analisti della sicurezza, i proprietari delle applicazioni e il team di leadership della sicurezza.

Gli esempi per le parti interessate esterne includono persone provenienti da fornitori di software indipendenti (ISV) e fornitori di servizi gestiti (MSP) che si desidera includere in un processo di risposta agli incidenti.

Note

La configurazione del team di risposta agli incidenti non concede automaticamente ai membri del team l'accesso a risorse di servizio come iscrizioni e casi. È possibile utilizzare policy AWS gestite per AWS Security Incident Response concedere l'accesso in lettura e scrittura alle risorse. [Fai clic qui per saperne di più.](#)

I membri del team di risposta agli incidenti specificati a livello di iscrizione verranno aggiunti automaticamente a ogni caso. Puoi aggiungere o rimuovere singoli compagni di squadra in qualsiasi momento dopo la creazione di un caso.

Il team di risposta agli incidenti riceverà una notifica via e-mail sugli eventi elencati nelle preferenze di [comunicazione](#).

Preferenze di comunicazione

Configura le tue preferenze di comunicazione per controllare il modo in cui ricevi le notifiche e interagisci con il sistema di risposta agli incidenti durante gli incidenti di sicurezza.

Gestisci le preferenze di comunicazione del team

Puoi configurare le preferenze di comunicazione per i singoli membri del tuo team di risposta agli incidenti dalla pagina della dashboard.

Segui questi passaggi per gestire le impostazioni di comunicazione dei membri del team:

1. Vai alla pagina del team di risposta agli incidenti dalla tua dashboard
2. Esegui una delle seguenti operazioni:
 - Per aggiornare un membro del team esistente: seleziona il collega di cui desideri modificare le preferenze di comunicazione, quindi scegli Modifica
 - Per aggiungere un nuovo membro del team: scegli Aggiungi
3. Nella parte inferiore del modulo vedrai Comunicazioni
 - a. Seleziona le caselle di controllo relative alle comunicazioni che desideri ricevere
 - b. Deseleziona le caselle di controllo relative alle comunicazioni che non desideri ricevere

Communications

Select communication type

- Case acknowledged
- Case assignee updated
- Case attachment scan failed
- Case attachment scan succeeded
- Case attachment uploaded
- Case attachment URL uploaded
- Case break glass
- Case closed
- Case comment added
- Case comment updated
- Case created
- Case entitlement updated
- Case owner updated
- Case pending customer action reminder
- Case updated
Notifications about cases, such as new case creations, new case updates, and case closure.
- Case updated to service managed
- Case update case status
- Deregister delegated administrator
- Disable AWS service access
- Membership cancelled
- Membership created
- Membership updated
Notifications about changes to membership, such as membership account updates and cancellations.
- Register delegated administrator

4. Salva le modifiche

Incident Response Team

▼ Set up your Incident Response Team

Add members and grant permissions

Configure your team by adding key stakeholders from within and outside your organization. This can include stakeholders such as legal, application leads, product managers, or 3rd party security services.

Receive email notifications by default

Team members automatically added to any case that is being created by default. These members can be removed before creating the case. Team members are automatically notified for any updates to service membership.

Teammates (2/10)

You can specify up to 10 members in your Incident Response Team. Additional members can be added for individual cases.

Name	Job title	Email	Communications
<input type="checkbox"/> John	Security Engineer	john@security-engineer.com	<ul style="list-style-type: none"> • Case updated • Case acknowledged • Case status updated • Case comment added Show more (+11)
<input type="checkbox"/> Sarah	Security Manager	sarah@security-manager.com	<ul style="list-style-type: none"> • Case created • Case updated • Case acknowledged • Case status updated Show more (+12)

Impostazioni di comunicazione predefinite

Per impostazione predefinita, i membri del team di risposta agli incidenti avranno tutte le comunicazioni abilitate. Puoi modificare queste impostazioni in qualsiasi momento utilizzando i passaggi precedenti.

Opzioni di comunicazione

Le tue preferenze di comunicazione controllano il modo in cui interagisci con il sistema di risposta agli incidenti e il modo in cui ti vengono inviate le notifiche durante gli incidenti di sicurezza.

Note

Queste preferenze si applicano a tutte le comunicazioni future all'interno del sistema Security Incident Response. È possibile modificare queste impostazioni in qualsiasi momento ripetendo i passaggi precedenti.

Associazione dell'account a AWS Organizations

Quando abiliti AWS Security Incident Response, ti verrà data la possibilità di selezionare l'intera organizzazione o unità organizzative specifiche (OUs). Se OUs vengono selezionati determinati account, l'iscrizione coprirà solo gli account che rientrano tra quelli selezionati OUs. Se viene selezionata l'intera organizzazione, l'iscrizione coprirà tutti gli account all'interno dell'organizzazione.

Per maggiori dettagli, consulta [Gestire AWS Security Incident Response gli account con AWS Organizations](#).

Gestione della copertura dell'abbonamento

Puoi modificare l'opzione di copertura dell'abbonamento in qualsiasi momento, incluso il passaggio dalla copertura a livello di organizzazione a quella specifica. OUs

Aggiornamento delle associazioni OU

Per gestire la copertura dei tuoi abbonamenti:

1. Vai alla pagina delle impostazioni di associazione degli account
2. Seleziona Aggiungi OUs per selezionare OUs quello che desideri associare alla tua iscrizione
3. Seleziona OUs quello che desideri associare alla tua iscrizione
4. Fai clic su Aggiorna associazione per salvare l'associazione OU nella tua iscrizione

Dopo aver aggiornato le associazioni, puoi tornare alla stessa pagina e rimuovere quelle OUs che desideri dissociare dalla tua iscrizione. Questa flessibilità si applica anche se inizialmente hai

selezionato l'intera organizzazione: in seguito puoi aggiornare la tua iscrizione in modo che copra solo informazioni specifiche OUs senza annullare e riattivare il servizio.

Per ulteriori informazioni, consulta [Gestire l'appartenenza](#) con le unità organizzative (). OUs

Considerazioni importanti

Account che si trovano direttamente nella cartella principale: quando si seleziona un tipo specifico OUs di appartenenza, gli account che si trovano direttamente nella cartella principale dell'organizzazione (che non fanno parte di alcuna unità organizzativa) non verranno associati all'iscrizione. Per includere questi account nella copertura dei soci, è necessario prima aggiungerli a un'unità organizzativa, quindi associare tale unità organizzativa alla propria iscrizione.

Note

Miglioriamo continuamente l'esperienza utente dell'associazione OU per rendere il processo più intuitivo e autoesplicativo.

Monitoraggio e indagine

AWS Security Incident Response esamina e classifica gli avvisi di sicurezza di Amazon GuardDuty AWS Security Hub CSPM, quindi configura le regole di soppressione in base al tuo ambiente per prevenire avvisi non necessari. Il team di AWS Security Incident Response Engineering (SIRE) analizza i risultati e li elabora rapidamente e li guida per contenere rapidamente i potenziali problemi. Se lo desideri, puoi concedere l'AWS Security Incident Response autorizzazione a implementare azioni di contenimento per tuo conto.

AWS Security Incident Response si allinea alla Guida alla gestione degli eventi di [sicurezza informatica NIST 800-61r2 per la risposta agli eventi di sicurezza](#). Allineandosi a questo standard di settore, AWS Security Incident Response fornisce un approccio coerente alla gestione degli eventi di sicurezza e rispetta le migliori pratiche per proteggere e rispondere agli eventi di sicurezza nell'ambiente in uso. AWS

Quando AWS Security Incident Response identifica un avviso di sicurezza o richiedi assistenza di sicurezza, il SIRE effettua un'indagine. AWS Il team raccoglie gli eventi di registro e i dati di servizio, come GuardDuty avvisi, triage e analizza tali dati, esegue attività di correzione e contenimento e fornisce report post-incidente.

Indice

- [Preparazione](#)
- [Rileva e analizza](#)
- [Agente investigativo AI](#)
- [Contenere](#)
- [Sradicare](#)
- [Ripristino](#)
- [Segnalazione post incidente](#)

Preparazione

Il AWS Security Incident Response team indaga e collabora con voi durante tutto il ciclo di vita della risposta agli eventi di sicurezza. Si consiglia di configurare questo team e assegnare le autorizzazioni necessarie prima che si verifichi un evento di sicurezza.

Rileva e analizza

Segnalazione di un evento

Puoi segnalare un evento di sicurezza tramite il AWS Security Incident Response portale. È importante non aspettare durante un evento di sicurezza. AWS Security Incident Response utilizza tecniche automatizzate e manuali per indagare sugli eventi di sicurezza, analizzare i log e cercare schemi anomali. La collaborazione e la comprensione dell'ambiente in uso accelerano questa analisi.

Abilitazione delle fonti di rilevamento supportate

Note

AWS Security Incident Response i costi del servizio non includono l'utilizzo e altri costi e tariffe associati alle fonti di rilevamento o all'uso di altri AWS servizi supportate. Per i dettagli sui costi, consulta le pagine delle singole funzionalità o dei servizi.

Amazon GuardDuty

Per abilitarlo GuardDuty in tutta la tua organizzazione, consulta la [Setting up GuardDuty](#) sezione della [Amazon GuardDuty User Guide](#).

Ti consigliamo vivamente di abilitare tutte GuardDuty le funzionalità supportate Regioni AWS. Ciò consente di GuardDuty generare informazioni su attività non autorizzate o insolite anche in aree che

non vengono utilizzate attivamente. Per ulteriori informazioni, consulta le [GuardDuty regioni e gli endpoint Amazon](#)

Enabling GuardDuty fornisce AWS Security Incident Response l'accesso ai dati critici di rilevamento delle minacce, migliorando la sua capacità di identificare e rispondere a potenziali problemi di sicurezza nel tuo AWS ambiente.

AWS Security Hub CSPM

Security Hub CSPM può acquisire i risultati di sicurezza da diversi AWS servizi e soluzioni di sicurezza di terze parti supportate. Queste integrazioni possono aiutare a AWS Security Incident Response monitorare e analizzare i risultati provenienti da altri strumenti di rilevamento.

Per abilitare l'integrazione di Security Hub CSPM with Organizations, consulta la Guida per l'[AWS Security Hub CSPM utente](#).

Esistono diversi modi per abilitare le integrazioni su Security Hub CSPM. Per le integrazioni di prodotti di terze parti, potrebbe essere necessario acquistare l'integrazione da e quindi Marketplace AWS configurare l'integrazione. Le informazioni sull'integrazione forniscono collegamenti per completare queste attività. Scopri di più su [come abilitare AWS Security Hub CSPM le integrazioni](#).

AWS Security Incident Response può monitorare e analizzare i risultati dei seguenti strumenti quando sono integrati con AWS Security Hub CSPM:

- [CrowdStrike — CrowdStrike Falco](#)
- [Merletto — Merletto](#)
- [Trend Micro — Cloud One](#)

Abilitando queste integrazioni, è possibile migliorare in modo significativo la portata e l'efficacia delle capacità AWS Security Incident Response di monitoraggio e indagine.

Rilevamento

Se la «Risposta proattiva» è abilitata https://docs.aws.amazon.com/security-ir/latest/userguide/setup_monitoring-and-investigation-workflows.html acquisisce i risultati di AWS Security Incident Response da Amazon e GuardDuty tramite EventBridge le regole di AWS Security Hub CSPM Amazon che vengono distribuite ai tuoi account durante l'onboarding.

AWS Security Incident Response archivia automaticamente GuardDuty i risultati di Amazon che durante il triage automatico sono determinati come benigni o associati all'attività prevista. Puoi

visualizzare i risultati archiviati nella GuardDuty console Amazon selezionando Archiviato dal filtro Status dei risultati. Per ulteriori informazioni, consulta [Visualizzazione dei risultati generati nella GuardDuty console](#) nella Amazon GuardDuty User Guide.

AWS Security Incident Response archivia automaticamente GuardDuty i risultati di Amazon che durante il triage automatico sono determinati come benigni o associati all'attività prevista. Questa archiviazione avviene solo per i risultati che sono stati valutati e il cui risultato è stato designato come «archivio». I risultati oggetto di indagine attiva rimangono visibili nella GuardDuty console Amazon anche dopo la conclusione di un'indagine. Puoi visualizzare i risultati archiviati nella GuardDuty console Amazon selezionando Archiviato dal filtro dei risultati. Per ulteriori informazioni sull'utilizzo dei risultati archiviati, consulta [Lavorare con i risultati](#) nella Amazon GuardDuty User Guide.

Quando AWS Security Hub CSPM acquisisce i risultati di sicurezza, il sistema aggiorna ogni risultato con una nota che indica che il triage automatico è iniziato. Lo stato del flusso di lavoro passa da NUOVO a NOTIFICATO, il che rimuove il risultato dalla visualizzazione predefinita dei AWS Security Hub CSPM risultati. Se il triage determina che un risultato è innocuo o associato all'attività prevista, il sistema aggiunge una nota al risultato e aggiorna lo stato del flusso di lavoro su SUPPRESSED.

Analisi: triage automatico

AWS Security Incident Response valuta automaticamente i risultati di sicurezza. Il processo di valutazione determina se l'attività rilevata rappresenta il comportamento previsto, analizzando i dati provenienti da più fonti, tra cui il payload di ricerca, i metadati dei AWS servizi, i dati di AWS registrazione e monitoraggio (come i log di flusso AWS CloudTrail VPC), l'intelligence AWS sulle minacce e il contesto che sei invitato a fornire sul tuo ambiente e su quello locale. AWS

Se il triage automatico determina che l'attività rilevata è prevista, il sistema non intraprende ulteriori azioni investigative.

Analisi: Incident Response Security Investigation

AWS Security Incident Response Engineering è un team globale e sempre disponibile di professionisti della sicurezza con esperienza nella risposta agli incidenti AWS di sicurezza. Se il triage automatizzato non è in grado di determinare se l'attività è prevista, AWS Security Incident Response Engineering si impegna a eseguire un'indagine di sicurezza. Se l'evento è stato acquisito da Security Hub, viene pubblicata una nota sul relativo risultato in cui si afferma che l'indagine di AWS Security Incident Response Engineering è in corso.

AWS Security Incident Response Engineering conduce un'indagine pratica sulla sicurezza analizzando i metadati di servizio aggiuntivi e l'intelligence sulle minacce, esaminando le informazioni

ricavate da scoperte e indagini precedenti nel vostro ambiente e applicando le competenze in materia di risposta agli incidenti. [A seconda delle preferenze di contenimento \(vedi Contenere\), AWS Security Incident Response Engineering può coinvolgere il team Incident Response dell'organizzazione attraverso un caso di Security Incident Response nella AWS Security Incident Response console per verificare se l'attività rilevata è prevista e autorizzata in risposta a un caso generato. AWS](#)

Comunicare

AWS Security Incident Response ti tiene informato durante le indagini di sicurezza interagendo con il tuo team di Incident Response attraverso un caso di Security Incident Response. Più membri di AWS Security Incident Response Engineering possono supportare un'indagine. La comunicazione può includere: conferma o notifica dell'avvio di un'indagine di sicurezza, creazione di un call bridge, analisi di elementi come i file di registro, richieste di conferma dell'attività prevista e condivisione dei risultati delle indagini.

Quando si coinvolge in AWS Security Incident Response modo proattivo il team Incident Response, viene creato un caso nell'account AWS Security Incident Response Membership, che centralizza le comunicazioni per tutti gli account dell'organizzazione in un unico posto. Questi casi contengono il prefisso «[Proactive case]» nel titolo, che li identifica come avviati da. AWS Security Incident Response Interagendo attivamente e fornendo risposte tempestive a queste comunicazioni, il tuo team di Incident Response può aiutarti AWS Security Incident Response a fare quanto segue:

- Garantisci una risposta rapida a veri incidenti di sicurezza.
- Comprendi il tuo ambiente e i comportamenti previsti.
- Riduci i rilevamenti di falsi positivi nel tempo.

L'efficacia di AWS Security Incident Response migliora con la collaborazione e si traduce in un AWS ambiente monitorato e sicuro in modo più efficace.

Aggiornamento dei risultati

AWS Security Incident Response gestisce i risultati in modo diverso a seconda della fonte e del risultato del triage.

Ottimizzazione del servizio

[Quando le quote di servizio del tuo account lo consentono, AWS Security Incident Response tenta di implementare una regola di GuardDuty soppressione di Amazon o una AWS Security Hub CSPM regola di automazione.](#) Queste regole eliminano i risultati futuri che corrispondono al tipo e all'origine

dell'attività autorizzata nota (ad esempio, indirizzo IP di origine, ASN, identità principale o risorsa). AWS Security Hub CSPM le regole vengono implementate con priorità 10, che consente di sostituire queste automazioni con regole autodefinitive, se necessario.

In questo modo, AWS Security Incident Response ottimizza le sorgenti di rilevamento in base al comportamento previsto nell'ambiente. AWS Il vostro Incident Response Team viene informato delle modifiche a questi set di regole e le modifiche vengono ripristinate su richiesta.

Agente investigativo AI

Panoramica di

L'agente investigativo basato sull'intelligenza artificiale collabora con clienti e AWS Security Incident Response ingegneri per accelerare le indagini di sicurezza. Quando un cliente crea un caso AWS supportato, l'agente si attiva automaticamente in parallelo al coinvolgimento dei tecnici del Security Incident Response, riducendo i tempi di risoluzione da giorni a ore.

Durante le escalation di clienti, i casi di Security Incident Response potrebbero essere creati da te o in modo proattivo da AWS Security Incident Response. Quando viene creato un nuovo caso AWS supportato, l'agente investigativo si attiva automaticamente. Puoi gestire tutti i casi tramite la console, l'API o EventBridge e le integrazioni Amazon.

Vantaggi principali

- **Indagine parallela:** l'agente collabora contemporaneamente con i soccorritori, fornendo sia automazione basata sull'intelligenza artificiale che competenze umane.
- **Raccolta automatica delle prove:** elimina l'analisi manuale dei log eseguendo interrogazioni automatiche su IAM AWS CloudTrail, Amazon EC2 e Cost Explorer.
- **Interfaccia in linguaggio naturale:** descrivi i problemi di sicurezza in un linguaggio semplice senza bisogno di esperienza nei AWS formati di log.
- **Risposta più rapida:** i riepiloghi delle indagini sono disponibili in pochi minuti nella scheda Indagine.
- **Verificabilità completa:** tutte le azioni degli agenti vengono registrate AWS CloudTrail sotto il ruolo `AWSserviceRoleForSupport`

Important

Questa funzionalità è disponibile solo per i AWS casi supportati. I casi autogestiti non includono funzionalità di indagine basata sull'intelligenza artificiale.

Come funziona

L'agente investigativo basato sull'intelligenza artificiale segue un flusso di lavoro strutturato durante l'analisi dei casi di sicurezza AWS supportati:

Workflow di indagine

1. Creazione del caso: il cliente crea un caso AWS supportato nella console Security Incident Response descrivendo il problema di sicurezza.
2. Attivazione parallela
 - I tecnici del Security Incident Response si occupano del caso.
 - Contemporaneamente, l'agente AI inizia il flusso di lavoro investigativo.
3. Domande contestuali (facoltative): l'agente può porre domande di chiarimento per raccogliere dettagli specifici:
 - Account interessato AWS IDs
 - Principali IAM coinvolti (utenti, ruoli, chiavi di accesso)
 - Identificatori di risorse specifici (bucket S3, istanze EC2,) ARNs
 - Intervallo di tempo in cui si verifica un'attività sospetta
4. Raccolta di prove: l'agente interroga AWS automaticamente le fonti di dati:
 - AWS CloudTrail— Chiamate e attività API associate all'incidente
 - IAM: autorizzazioni per utenti e ruoli, modifiche alle policy e creazione di nuove identità
 - Istanza Amazon EC2 APIs: informazioni sulle risorse di elaborazione, se coinvolte
 - Cost Explorer: metriche di costo e utilizzo per un consumo insolito di risorse
5. Analisi e correlazione: l'agente mette in correlazione le prove tra i servizi, identifica i modelli e crea una sequenza temporale degli eventi.
6. Generazione di un riepilogo: in pochi minuti, l'agente presenta un riepilogo completo dell'indagine nella scheda Indagine.

Note

Tutti i campi sono facoltativi. Se non viene fornita alcuna risposta entro 10 minuti, l'indagine viene avviata automaticamente. In alcuni casi, se sono già disponibili informazioni sufficienti, l'agente può saltare completamente le domande opzionali.

Accesso ai risultati delle indagini

Per visualizzare l'analisi dell'IA:

1. Accedi al tuo caso nella console Security Incident Response.
2. Seleziona la scheda Indagine.
3. Consulta il riepilogo dell'indagine con i risultati, la tempistica e il contesto.

Il riepilogo dell'agente investigativo di AI viene pubblicato automaticamente come commento nella sezione Comunicazione del caso, facilitandone la lettura insieme ad altri aggiornamenti del caso.

Accesso ai dati e autorizzazioni

L'agente investigativo AI utilizza il `AWSServiceRoleForSupport` Service-Linked Role per accedere alle risorse. AWS Questo ruolo fornisce le autorizzazioni di sola lettura necessarie per la raccolta delle prove.

Tutte le azioni eseguite dall'agente vengono registrate AWS CloudTrail, permettendo ai clienti di verificare esattamente a quali dati hanno avuto accesso durante l'indagine. Nei AWS CloudTrail log, queste azioni sono attribuite a `AWSServiceRoleForSupport`

Prerequisiti

Prima di utilizzare le funzionalità di indagine basate sull'intelligenza artificiale, assicurati quanto segue:

Configurazione richiesta

- AWS Security Incident Response abilitato: il servizio deve essere abilitato tramite l'account AWS Organizations di gestione.
- AWS tipo di caso supportato: l'indagine basata sull'IA è disponibile solo per i casi AWS supportati (non per i casi autogestiti).
- `AWSServiceRoleForSupport`— Questo ruolo collegato al servizio viene creato automaticamente e fornisce le autorizzazioni necessarie all'agente investigativo.

Autorizzazioni richieste

Per creare casi AWS supportati e accedere ai risultati delle indagini, il responsabile IAM necessita delle seguenti autorizzazioni:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "security-ir:CreateCase",
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:UpdateCase"
      ],
      "Resource": "*"
    }
  ]
}
```

Utilizzo dell'agente investigativo

L'agente investigativo basato sull'intelligenza artificiale si attiva automaticamente durante la creazione di un AWS caso supportato.

Per monitorare i progressi delle indagini sull'intelligenza artificiale

1. Apri la custodia nella AWS Security Incident Response console.
2. Scegli la scheda Indagine.
3. Visualizza lo stato dell'indagine (In corso o Completata).
4. Una volta completata, consulta il riepilogo completo dell'indagine con risultati, tempistica e raccomandazioni.

Divulgazione responsabile dell'IA

I riepiloghi delle indagini vengono generati utilizzando funzionalità di intelligenza AWS artificiale generativa. Sei responsabile della valutazione delle raccomandazioni generate dall'intelligenza artificiale nel tuo contesto specifico, dell'implementazione di meccanismi di supervisione appropriati, della verifica dei risultati in modo indipendente e del mantenimento della supervisione umana di tutte le decisioni di sicurezza.

Utilizzo dei dati dei clienti

Al Investigative Agent non utilizza i dati dei clienti per la formazione dei modelli e non condivide i dati dei clienti con terze parti.

Contenere

AWS Security Incident Response collabora con te per contenere gli eventi. Puoi configurare il servizio in modo che intraprenda azioni di contenimento proattive nel tuo account in risposta ai risultati di sicurezza. [Puoi anche eseguire il contenimento da solo o in collaborazione con le tue relazioni con terze parti utilizzando i documenti SSM descritti in Azioni di contenimento supportate.](#)

Important

AWS Per impostazione predefinita, Security Incident Response non abilita le funzionalità di contenimento.

Per abilitare le funzionalità di contenimento proattivo sono necessari due passaggi:

1. Concedi le autorizzazioni necessarie al servizio utilizzando i ruoli IAM. Puoi creare questi ruoli singolarmente per account o per l'intera organizzazione utilizzando gli AWS CloudFormation stackset, che creano i ruoli richiesti.
2. Definisci le tue preferenze di contenimento per account o in tutta l'organizzazione per autorizzare azioni di contenimento proattive. Le preferenze a livello di account sostituiscono le preferenze a livello di organizzazione. Ciò può essere fatto creando un AWS Support Case (tecnico: Security Incident Response Service/Altro). Le preferenze di contenimento disponibili sono:
 - Approvazione richiesta (impostazione predefinita): non eseguire il contenimento proattivo di alcuna risorsa senza un'autorizzazione esplicita su base case-by-case
 - Contenimento confermato: esegui il contenimento proattivo di una risorsa confermata compromessa.
 - Contenimento sospetto: esegui il contenimento proattivo di una risorsa con un'alta probabilità che sia stata compromessa, in base all'analisi eseguita da Security Incident Response Engineering. AWS

Processo decisionale in materia di contenimento

Una parte essenziale del contenimento è il processo decisionale, ad esempio se spegnere un sistema, isolare una risorsa dalla rete, disattivare l'accesso o terminare le sessioni. Queste decisioni sono semplificate quando esistono strategie e procedure predeterminate per contenere l'evento. AWS Security Incident Response fornisce la strategia di contenimento, vi informa sul potenziale impatto e vi guida nell'implementazione della soluzione solo dopo aver considerato e accettato i rischi connessi.

Azioni di contenimento supportate

AWS Security Incident Response esegue le azioni di contenimento supportate per conto dell'utente per accelerare la risposta e ridurre il tempo a disposizione di un autore della minaccia per causare potenzialmente danni all'ambiente. Questa funzionalità consente una mitigazione più rapida delle minacce identificate, minimizzando il potenziale impatto e migliorando il livello di sicurezza generale. Esistono diverse opzioni di contenimento a seconda delle risorse oggetto di analisi. Le azioni di contenimento supportate sono descritte nelle sottosezioni seguenti.

Contenimento EC2

L'automazione del `AWSSupport-ContainEC2Instance` contenimento esegue un contenimento di rete reversibile di un'istanza EC2, lasciando l'istanza intatta e funzionante, ma isolandola da qualsiasi nuova attività di rete e impedendole di comunicare con le risorse all'interno e all'esterno del VPC.

Important

È importante notare che le connessioni tracciate esistenti non verranno interrotte a seguito della modifica dei gruppi di sicurezza: solo il traffico futuro verrà effettivamente bloccato dal nuovo gruppo di sicurezza e da questo documento SSM. Ulteriori informazioni sono disponibili nella sezione relativa al [contenimento dei sorgenti](#) della guida tecnica al servizio.

Contenimento IAM

L'automazione del `AWSSupport-ContainIAMPrincipal` contenimento esegue un contenimento di rete reversibile di un utente o ruolo IAM, lasciando l'utente o il ruolo in IAM, ma isolandolo dalla comunicazione con le risorse all'interno dell'account.

Contenimento S3

L'automazione del `AWSSupport-ContainS3Resource` contenimento esegue un contenimento reversibile di un bucket S3, lasciando gli oggetti nel bucket e isolando il bucket o l'oggetto Amazon S3 modificandone le politiche di accesso.

Sviluppo di strategie di contenimento

AWS Security Incident Response vi incoraggia a prendere in considerazione strategie di contenimento per ogni tipo di evento importante che rientrino nella vostra propensione al rischio. Documenta criteri chiari per facilitare il processo decisionale durante un evento. I criteri da considerare includono:

- Potenziali danni alle risorse
- Conservazione delle prove e requisiti normativi
- Indisponibilità del servizio (ad esempio, connettività di rete, servizi forniti a parti esterne)
- Tempo e risorse necessari per implementare la strategia
- Efficacia della strategia (ad esempio, contenimento parziale o totale)
- Permanenza della soluzione (ad esempio, reversibile o irreversibile)
- Durata della soluzione (ad esempio, soluzione alternativa di emergenza, soluzione temporanea, soluzione permanente)

Applica controlli di sicurezza in grado di ridurre i rischi e concedere il tempo necessario per definire e implementare una strategia di contenimento più efficace.

Approccio di contenimento graduale

AWS Security Incident Response consiglia un approccio graduale per raggiungere un contenimento efficiente ed efficace, che preveda strategie a breve e lungo termine basate sul tipo di risorsa.

Strategia di contenimento

È in grado di AWS Security Incident Response identificare l'ambito dell'evento di sicurezza?

- In caso affermativo, identifica tutte le risorse (utenti, sistemi, risorse).
- In caso negativo, esaminate parallelamente all'esecuzione del passaggio successivo sulle risorse identificate.

La risorsa può essere isolata?

- In caso affermativo, procedi a isolare le risorse interessate.
- In caso negativo, collabora con i proprietari e i gestori del sistema per determinare le ulteriori azioni necessarie per contenere il problema.

Tutte le risorse interessate sono isolate dalle risorse non interessate?

- In caso affermativo, procedi con il passaggio successivo.
- In caso negativo, continuate a isolare le risorse interessate per completare il contenimento a breve termine ed evitare che l'evento si aggravi ulteriormente.

Backup del sistema

Le copie di backup dei sistemi interessati sono state create per ulteriori analisi?

Le copie forensi sono crittografate e archiviate in un luogo sicuro?

- In caso affermativo, procedi con il passaggio successivo.
- In caso negativo, crittografa le immagini forensi, quindi conservale in un luogo sicuro per evitare utilizzi accidentali, danni e manomissioni.

Invia le preferenze di contenimento

[Per configurare le preferenze di contenimento per il tuo account o la tua organizzazione, crea un Supporto AWS caso.](#)

Nel caso di assistenza, specifica le seguenti informazioni:

Una volta configurato, AWS Security Incident Response esegue le azioni di contenimento autorizzate durante gli incidenti di sicurezza attivi per proteggere l'ambiente.

- Il tuo AWS Organizations ID o l'account specifico IDs in cui le azioni di contenimento devono essere autorizzate.
- La tua opzione di contenimento preferita.

Note

AWS Security Incident Response esegue azioni di contenimento solo se configurate con le preferenze appropriate e dopo aver distribuito quelle richieste per concedere le autorizzazioni necessarie AWS CloudFormation StackSet .

Sradicare

Durante la fase di eradicazione, è importante identificare e risolvere tutti gli account, le risorse e le istanze interessati, ad esempio eliminando il malware, rimuovendo gli account utente compromessi e mitigando le vulnerabilità scoperte, per applicare una correzione uniforme in tutto l'ambiente.

È consigliabile utilizzare un approccio graduale all'eradicazione e al ripristino e dare priorità alle fasi di riparazione. Lo scopo delle fasi iniziali è aumentare rapidamente la sicurezza complessiva (da

giorni a settimane) con modifiche di alto valore per prevenire eventi futuri. Le fasi successive possono concentrarsi su cambiamenti a lungo termine (ad esempio, modifiche all'infrastruttura) e sul lavoro in corso per mantenere l'azienda il più sicura possibile. Ogni caso è unico e i tecnici del AWS Security Incident Response collaboreranno con voi per valutare le azioni necessarie.

Considera i seguenti aspetti:

- È possibile reimpostare l'immagine del sistema e rafforzarlo con patch o altre contromisure per prevenire o ridurre il rischio di attacchi?
- È possibile sostituire il sistema infetto con una nuova istanza o risorsa, garantendo una linea di base pulita e allo stesso tempo eliminando l'elemento infetto?
- Avete rimosso tutto il malware e gli altri artefatti lasciati dall'uso non autorizzato e rafforzato i sistemi interessati da ulteriori attacchi?
- È necessario effettuare analisi forensi sulle risorse interessate?

Ripristino

AWS Security Incident Response fornisce indicazioni per aiutare a ripristinare il normale funzionamento dei sistemi, confermare che funzionino correttamente e correggere eventuali vulnerabilità per prevenire eventi simili in futuro. AWS Security Incident Response non aiuta direttamente il ripristino dei sistemi. Le considerazioni chiave includono:

- I sistemi interessati sono aggiornati e rafforzati contro il recente attacco?
- Qual è la tempistica possibile per ripristinare i sistemi in produzione?
- Quali strumenti utilizzerai per testare, monitorare e verificare i sistemi ripristinati?

Segnalazione post incidente

AWS Security Incident Response fornisce un riepilogo dell'evento dopo la conclusione delle attività di sicurezza tra il tuo team e il nostro.

Alla fine di ogni mese, il AWS Security Incident Response servizio invierà report mensili al punto di contatto principale di ogni cliente tramite e-mail. I report verranno forniti in formato PDF utilizzando le metriche descritte di seguito. I clienti riceveranno un rapporto per persona. AWS Organizations

Metriche del caso

- Casi creati

- Nome della dimensione: Tipo
- Valori delle dimensioni: AWS supportati, supportati automaticamente
- Unità: numero
- Descrizione: il numero di casi creati.
- Casi chiusi
 - Nome dimensione: Tipo
 - Valori delle dimensioni: AWS supportati, autogestiti
 - Unità: numero
 - Descrizione: una misura del numero totale di casi chiusi.
- Casi aperti
 - Nome dimensione: Tipo
 - Valori delle dimensioni: AWS supportati, supportati automaticamente
 - Unità: numero
 - Descrizione: il numero di casi aperti.

Metriche di triaging

- Risultati ricevuti
 - Unità: numero
 - Descrizione: Il numero di risultati inviati al triaging.
- Risultati archiviati
 - Unità: numero
 - Descrizione: Il numero di risultati archiviati dopo l'elaborazione senza indagini manuali.
- Risultati esaminati manualmente
 - Unità: numero
 - Descrizione: Il numero di risultati ottenuti con un'indagine manuale.
- Indagini archiviate
 - Unità: numero
 - Descrizione: il numero di indagini manuali che hanno prodotto falsi positivi e inviate per l'archiviazione

- **Unità:** numero
- **Descrizione:** Il numero di indagini manuali che hanno portato a un incidente di sicurezza

Casi

AWS Security Incident Response consente di creare due tipi di casi: casi AWS supportati o casi autogestiti.

Crea un caso AWS supportato

Puoi creare un caso AWS supportato AWS Security Incident Response tramite la Console, l'API o il AWS Command Line Interface. AWS i casi supportati consentono di ricevere supporto dai tecnici di Security Incident Response.

Important

I casi di dimostrazione/simulazione verranno chiusi dopo un periodo di 90 giorni.

Note

AWS I tecnici di Security Incident Response risponderanno al tuo caso entro 15 minuti. Il tempo di risposta si riferisce alla prima risposta dei tecnici del AWS Security Incident Response. Faremo ogni ragionevole sforzo per rispondere alla richiesta iniziale entro questo lasso di tempo. Questo tempo di risposta non si applica alle risposte successive.

Note

È possibile creare casi AWS supportati non solo per incidenti e indagini di sicurezza attivi, ma anche per domande sulle funzionalità di AWS Security Incident Response. Ciò include domande sulle regole di GuardDuty soppressione, sulle configurazioni di valutazione degli avvisi, sui flussi di lavoro di risposta proattiva e indicazioni generali sul livello di sicurezza. Seleziona il tipo di caso Investigations and Inquiries per questi scopi.

Quando contattare AWS Security Incident Response

Puoi contattare AWS Security Incident Response per vari scopi a seconda delle tue esigenze. La tabella seguente descrive i diversi scenari e il metodo di contatto appropriato per ciascuno di essi.

Scenario	Quando usare	Tempo di risposta	Tipo di caso
Incidente di sicurezza attiva	Stai riscontrando un incidente di sicurezza urgente che richiede assistenza e servizi di risposta immediata	15 minuti (prima risposta)	Incidente di sicurezza attiva
Indagine	Hai percepito un incidente di sicurezza e hai bisogno di assistenza per l'analisi dei log e la conferma secondaria dell'indagine sulla risposta all'incidente	15 minuti (prima risposta)	Indagini e richieste
Richieste e linee guida	Hai domande sui GuardDuty risultati di Amazon, sulle regole di soppressione, sulle configurazioni di triaging degli avvisi, sui flussi di lavoro di risposta proattiva o sulla posizione di sicurezza generale relativa alle funzionalità AWS Security Incident Response	15 minuti (prima risposta)	Indagini e richieste
Problemi di onboarding	Stai riscontrando problemi tecnici durante il processo di onboarding per Security Incident Response AWS	Varia in base al piano di supporto	Supporto AWS caso

Per tutti i casi AWS supportati (Active Security Incident and Investigations and Inquiries), i tecnici di AWS Security Incident Response risponderanno entro 15 minuti alla prima risposta. Questo tempo di risposta si applica solo al contatto iniziale e non si applica alle risposte successive.

L'esempio seguente riguarda l'uso della console.

1. Accedi AWS Security Incident Response tramite Console di gestione AWS.
2. Scegli Crea caso
3. Scegli Risolvi caso con AWS
4. Seleziona il tipo di richiesta
 - a. Active Security Incident: questo tipo è destinato al supporto e ai servizi di risposta agli incidenti urgenti.
 - b. Indagini e richieste: utilizzate questo tipo per gli incidenti di sicurezza percepiti, in cui AWS i tecnici del Security Incident Response possono fornire assistenza nell'analisi dei log e nella conferma secondaria delle indagini sulla risposta agli incidenti. È inoltre possibile utilizzare questo tipo per domande su GuardDuty risultati, regole di soppressione, configurazioni di classificazione degli avvisi, flussi di lavoro di risposta proattiva e domande generali sulla posizione di sicurezza relative alle funzionalità di Security Incident Response. AWS
5. Imposta la data di inizio stimata sulla data del primo indicatore dell'incidente. Ad esempio, quando hai riscontrato un comportamento anomalo per la prima volta o quando hai ricevuto il primo avviso di sicurezza correlato.
6. Definisci un titolo per il caso
7. Fornisci una descrizione dettagliata del caso. Considerate i seguenti aspetti che possono aiutare i soccorritori a risolvere il caso:
 - a. Che cos'è successo?
 - b. Chi ha scoperto e segnalato l'incidente?
 - c. Chi è interessato dal caso?
 - d. Qual è l'impatto noto?
 - e. Qual è l'urgenza di questo caso?
 - f. Aggiungine uno o più Account AWS IDs che rientrano nell'ambito del caso.
8. Aggiungi dettagli opzionali del caso:
 - a. Seleziona i servizi principali interessati dall'elenco a discesa.
 - b. Seleziona le principali regioni interessate dall'elenco a discesa.

- c. Aggiungi uno o più indirizzi IP degli autori delle minacce che hai identificato nell'ambito di questo caso.
9. Aggiungi opzionali addetti alla risposta agli incidenti aggiuntivi al caso che riceveranno le notifiche. Per aggiungere una persona, procedi come segue:
- a. Aggiungi un indirizzo email.
 - b. Aggiungi un nome e cognome opzionali.
 - c. Scegli Aggiungi nuovo per aggiungere un'altra persona.
 - d. Per rimuovere una persona, scegli l'opzione Rimuovi relativa a una persona.
 - e. Scegli Aggiungi per aggiungere tutte le persone elencate al caso.
 - i. Puoi selezionare più persone e scegliere Rimuovi per eliminarle dall'elenco.
10. Aggiungi tag opzionali alla custodia.
- a. Per aggiungere un tag, procedere come segue:
 - b. Scegli Aggiungi nuovo tag.
 - c. Per Chiave, inserisci il nome del tag.
 - d. In Valore, immetti il valore del tag.
 - e. Per rimuovere un tag, seleziona l'opzione Rimuovi per quel tag.

Dopo la creazione di un caso AWS supportato, i tecnici di AWS Security Incident Response e il team di risposta agli incidenti vengono immediatamente informati.

Per creare un caso AWS supportato da un'indagine basata sull'intelligenza artificiale

1. Apri la AWS Security Incident Response console all'indirizzo console.aws.amazon.com/.
2. Scegli Casi dal pannello di navigazione.
3. Scegli Crea caso.
4. Per Tipo di custodia, seleziona AWS-case supportate.
5. Fornisci i dettagli del caso, tra cui titolo, data di inizio dell'incidente e ID AWS dell'account interessato.
6. Nella sezione Descrivi l'evento di sicurezza, fornisci una descrizione completa dell'incidente.
7. Fornisci informazioni aggiuntive sui AWS servizi interessati, sulle regioni e su altri dettagli pertinenti.
8. Scegli Crea caso.

Dopo la creazione del caso, sia gli ingegneri di Security Incident Response che l'agente AI iniziano a lavorare contemporaneamente.

Per rispondere a domande di chiarimento sull'IA (opzionale)

1. Vai alla scheda Indagine relativa al tuo caso.
2. Esamina tutte le domande di chiarimento presentate dall'agente AI.
3. Rispondi alle domande o scegli Salta se preferisci non rispondere.
4. Scegli Invia per continuare. Tutti i campi sono facoltativi.

Divulgazione responsabile dell'IA

I riepiloghi delle indagini vengono generati utilizzando funzionalità di intelligenza AWS artificiale generativa. Sei responsabile della valutazione delle raccomandazioni generate dall'intelligenza artificiale nel tuo contesto specifico, dell'implementazione di meccanismi di supervisione appropriati, della verifica dei risultati in modo indipendente e del mantenimento della supervisione umana di tutte le decisioni di sicurezza.

Crea un caso autogestito

Puoi creare un modulo autogestito AWS Security Incident Response tramite la console, l'API o AWS Command Line Interface. Questo tipo di caso NON coinvolge i tecnici del AWS Security Incident Response. L'esempio seguente riguarda l'uso della console.

1. Accedi AWS Security Incident Response tramite l' Console di gestione AWS indirizzo <https://console.aws.amazon.com/security-ir/>.
2. Scegliere Create Case (Crea caso).
3. Scegli Risolvi il caso con il mio team di risposta agli incidenti.
4. Imposta la data di inizio stimata sulla data del primo indicatore dell'incidente. Ad esempio, quando hai riscontrato un comportamento anomalo per la prima volta o quando hai ricevuto il primo avviso di sicurezza correlato.
5. Definite un titolo per il caso. Si consiglia di includere i dati nel titolo del caso, come suggerito quando si seleziona l'opzione Genera titolo.
6. Inserisci Account AWS IDs che fanno parte del caso. Per aggiungere un ID account, procedi come segue:
 - a. Inserisci l'ID dell'account a 12 cifre e scegli Aggiungi account.

- b. Per rimuovere un account, scegli Rimuovi accanto all'account che desideri rimuovere dalla custodia.
7. Fornisci una descrizione dettagliata del caso.
- a. Considerate i seguenti aspetti che possono aiutare i soccorritori a risolvere il caso:
 - i. Che cos'è successo?
 - ii. Chi ha scoperto e segnalato l'incidente?
 - iii. Chi è interessato dal caso?
 - iv. Qual è l'impatto noto?
 - v. Qual è l'urgenza di questo caso?
8. Aggiungi dettagli opzionali sul caso:
- a. Seleziona i servizi principali interessati dall'elenco a discesa.
 - b. Seleziona le principali regioni interessate dall'elenco a discesa.
 - c. Aggiungi uno o più indirizzi IP degli autori delle minacce che hai identificato nell'ambito di questo caso.
9. Aggiungi opzionali addetti alla risposta agli incidenti aggiuntivi al caso che riceveranno le notifiche. Per aggiungere una persona, procedi come segue:
- a. Aggiungi un indirizzo email.
 - b. Aggiungi un nome e cognome opzionali.
 - c. Scegli Aggiungi nuovo per aggiungere un'altra persona.
 - d. Per rimuovere una persona, scegli l'opzione Rimuovi relativa a una persona.
 - e. Scegli Aggiungi per aggiungere tutte le persone elencate al caso. Puoi selezionare più persone e scegliere Rimuovi per eliminarle dall'elenco.
10. Aggiungi tag opzionali alla custodia. Per aggiungere un tag, procedere come segue:
- a. Scegli Aggiungi nuovo tag.
 - b. Per Chiave, inserisci il nome del tag.
 - c. In Valore, immetti il valore del tag.
 - d. Per rimuovere un tag, seleziona l'opzione Rimuovi per quel tag.

Il team di risposta agli incidenti riceverà una notifica via e-mail dopo la creazione del caso.

Collaborazione con i tecnici AWS di Security Incident Respon

Dopo aver aperto un caso di incidente di sicurezza, i tecnici del AWS Security Incident Response iniziano a lavorare sull'incidente. Questa sezione spiega cosa aspettarsi durante l'indagine e come collaborare efficacemente con il nostro team.

Cosa aspettarsi dai tecnici del AWS Security Incident Response

Quando apri un caso AWS supportato, all'incidente viene assegnato un tecnico del Security Incident Response. Il soccorritore assegnato si occuperà di:

- Rivedi le informazioni iniziali che hai fornito nel caso
- Analizza i registri AWS di servizio e i risultati di sicurezza pertinenti
- Identifica la portata e l'impatto dell'incidente di sicurezza
- Sviluppa un piano di indagine e risposta personalizzato in base alla tua situazione

Tempi di risposta: l'obiettivo del livello di servizio (SLO) per il riconoscimento di nuovi casi da parte degli AWS Security Incident Response ingegneri è entro 15 minuti. La tempistica della valutazione iniziale potrebbe variare in base alla gravità e alla complessità dei casi. Se i AWS Security Incident Response tecnici non ricevono una risposta o informazioni critiche da te entro 5 giorni lavorativi, il caso è chiuso.

Workflow di indagine

AWS Gli ingegneri di Security Incident Response seguono un processo strutturato di risposta agli incidenti allineato al framework NIST 800-61r2. Durante la tua indagine, puoi aspettarti le seguenti fasi:

1. Valutazione iniziale: i tecnici del Security Incident Response esaminano i dettagli del caso e confermano la portata dell'incidente
2. Indagine: i tecnici del Security Incident Response analizzano i log, identificano gli indicatori di compromissione e determinano la causa principale
3. Contenimento: gli ingegneri del Security Incident Response consigliano azioni per limitare l'impatto dell'incidente
4. Eradicazione e ripristino: gli ingegneri di Security Incident Response aiutano a rimuovere le minacce e ripristinare le normali operazioni
5. Revisione post-incidente: gli ingegneri di Security Incident Response forniscono risultati e raccomandazioni per prevenire incidenti futuri

Durante queste fasi, il tecnico del Security Incident Response ti tiene informato tramite gli aggiornamenti dei casi e può richiedere ulteriori informazioni o azioni da parte tua.

I tecnici di Information Security Incident Response possono richiedere

Per indagare efficacemente sull'incidente, i tecnici del AWS Security Incident Response potrebbero chiederti di fornire:

- **Dettagli sulla cronologia:** la data in cui hai rilevato per la prima volta l'incidente e tutti gli eventi rilevanti che lo hanno preceduto
- **Risorse interessate:** AWS account IDs, servizi, regioni e risorse ARNs specifici coinvolti
- **Informazioni di accesso:** dettagli su chi ha accesso alle risorse interessate ed eventuali modifiche recenti all'accesso
- **Contesto aziendale:** come vengono utilizzate le risorse interessate e potenziale impatto aziendale
- **Registri e prove:** registri, schermate o artefatti aggiuntivi che possono aiutare le indagini
- **Autorizzazione:** approvazione per eseguire specifiche azioni di contenimento o riparazione per conto dell'utente

Il tecnico addetto alla Security Incident Response spiegherà perché ogni informazione è necessaria e in che modo aiuta l'indagine.

Le migliori pratiche di comunicazione

Una comunicazione efficace accelera la risoluzione degli incidenti. Segui queste pratiche quando lavori con i tecnici del AWS Security Incident Response:

- **Rispondi tempestivamente** alle richieste di informazioni del tuo tecnico di Security Incident Response
- **Fornisci informazioni complete** anche se non sei sicuro della loro rilevanza
- **Fai domande** se non comprendi una raccomandazione o hai bisogno di chiarimenti
- **Aggiorna il caso** con eventuali nuovi sviluppi o modifiche all'incidente
- **Designate un contatto principale** del vostro team che si coordini con i tecnici del Security Incident Response

⚠ Important

Se i AWS Security Incident Response tecnici non ricevono una risposta alle richieste di informazioni critiche entro 5 giorni lavorativi, ci adopereremo per chiudere il caso. Puoi riaprire un caso se diventano disponibili nuove informazioni.

Il tuo ruolo durante le indagini

Sebbene AWS Security Incident Response gli ingegneri guidino le indagini, la tua partecipazione è essenziale. Sei responsabile delle seguenti azioni:

- Fornire risposte tempestive alle richieste di informazioni
- Implementazione delle azioni di contenimento e riparazione consigliate nell'ambiente in uso AWS
- Autorizzazione dei tecnici di Security Incident Response a intraprendere azioni per conto dell'utente (se è stata abilitata la risposta proattiva)
- Coordinamento con i team interni (sicurezza, legale, conformità) secondo necessità
- Prendere decisioni aziendali sulle priorità e sui compromessi di risposta agli incidenti

AWS Security Incident Response gli ingegneri forniscono competenze e consigli, ma voi mantenete il controllo sulle AWS risorse e prendete decisioni definitive sulle azioni di risposta.

Chiusura della custodia

AWS Security Incident Response i tecnici chiudono la custodia quando:

- L'incidente è stato contenuto e risolto
- Tutti i risultati delle indagini sono stati condivisi con te
- Non è richiesta alcuna ulteriore assistenza tecnica da parte dei tecnici del Security Incident Response
- Richiedete la chiusura del caso

Prima di chiudere un caso, il tecnico del Security Incident Response fornisce un riepilogo dei risultati, delle azioni intraprese e delle raccomandazioni per migliorare il livello di sicurezza.

Se hai bisogno di ulteriore assistenza dopo la chiusura del caso, puoi aprire un nuovo caso o un nuovo contatto Supporto AWS.

Rispondere a un caso AWS generato

AWS Security Incident Response potrebbe creare una notifica o un caso in uscita quando devi agire o essere a conoscenza di qualcosa che potrebbe avere un impatto sul tuo account o sulle tue risorse. Ciò si verifica solo se hai abilitato i flussi di lavoro di risposta proattiva e triaging degli avvisi come parte dell'abbonamento.

Queste notifiche vengono visualizzate come casi di Security Incident Response con il prefisso «[Proactive case]» nella console. AWS Security Incident Response Per visualizzare e gestire questi casi, completa i seguenti passaggi:

- Aprire la console Security Incident Response all'indirizzo <https://console.aws.amazon.com/security-ir/>
- Scegli Casi.
- Vengono visualizzati tutti i casi, inclusi quelli con il prefisso «[Caso proattivo]».

Puoi aggiornare, risolvere e riaprire questi casi secondo necessità. È possibile comunicare direttamente con il AWS Security Incident Response team in questi casi, garantendo una gestione efficiente dei potenziali problemi di sicurezza.

Gestione dei casi

Indice

- [Modifica dello stato del caso](#)
- [Cambiare il resolver](#)
- [Action Items \(Attività\)](#)
- [Modifica di un caso](#)
- [Comunicazioni](#)
- [Permissions](#)
- [Allegati](#)
- [Tag](#)
- [Attività relative ai casi](#)
- [Chiusura di un caso](#)

Modifica dello stato del caso

Un caso si trova in uno dei seguenti stati:

- **Inviato:** questo è lo stato iniziale di un caso. I casi in questo stato sono stati presentati da un richiedente, ma non sono ancora in fase di elaborazione.
- **Rilevamento e analisi:** questo stato indica che un addetto alle operazioni di soccorso ha iniziato a lavorare sul caso. Questa fase include la raccolta dei dati, la valutazione dell'evento e l'esecuzione di analisi per creare conclusioni basate sui dati.
- **Contenimento, eliminazione e ripristino:** in questa situazione, il soccorritore ha identificato attività sospette che richiedono uno sforzo aggiuntivo per essere rimosse. Il responsabile della risposta agli incidenti fornirà consigli per l'analisi dei rischi aziendali e ulteriori azioni. Se hai abilitato le funzionalità di opt-in per il servizio, un addetto alla risposta agli AWS incidenti richiederà il tuo consenso per eseguire azioni di contenimento con i documenti SSM negli account interessati.
- **Attività post-incidente:** in questo stato l'evento di sicurezza principale è stato contenuto. L'obiettivo ora è ripristinare e riportare le operazioni aziendali alla normalità. Se il resolver del caso è supportato, viene fornita un'analisi riassuntiva e della causa principale AWS.
- **Chiuso:** questo è lo stato finale del flusso di lavoro. I casi con stato chiuso indicano che il lavoro è stato completato. I casi chiusi non possono essere riaperti, quindi assicurati che tutte le azioni siano complete prima di passare a questo stato.

Scegli Azione/Aggiorna stato per modificare lo stato del caso per i casi autogestiti. Per i casi AWS supportati, lo stato è impostato dai tecnici del AWS Security Incident Response.

Cambiare il resolver

Per i casi autogestiti, il team di risposta agli incidenti può richiedere assistenza a AWS Scegli Richiedi assistenza da AWS per cambiare il risolutore per questo caso. AWSUna volta aggiornato il caso a AWS Supportato, lo stato viene modificato in Inviato. La cronologia dei casi esistente sarà disponibile per i tecnici del AWS Security Incident Response. Una volta che AWS avrai richiesto assistenza, non potrai tornare a gestirla automaticamente.

Action Items (Attività)

Un tecnico del AWS Security Incident Response che si occupa del caso può richiedere azioni al team interno.

Le azioni che compaiono dopo la creazione di un caso includono:

- Richiesta di concessione delle autorizzazioni a un addetto alle operazioni di soccorso per accedere a un caso
- Richiesta di fornire ulteriori informazioni sul caso

Azioni da intraprendere quando un caso è pronto per essere chiuso:

- Richiesta di revisione del rapporto sul caso
- Richiesta di chiusura del caso

Modifica di un caso

Scegli Modifica per modificare i dettagli di un caso.

Per i casi AWS supportati e autogestiti:

È possibile modificare i seguenti dettagli del caso dopo la creazione di un caso:

- Titolo
- Description

Solo per i casi AWS supportati:

Puoi modificare i campi aggiuntivi:

- Tipo richiesta:
 - Active Security Incident: questo tipo è destinato al supporto e ai servizi di risposta agli incidenti urgenti.
 - Indagini: le indagini consentono di ottenere assistenza in caso di incidenti di sicurezza percepiti, mentre i tecnici del AWS Security Incident Response possono fornire assistenza nella registrazione e nella conferma secondaria dell'evento di sicurezza.
- Stima della data di inizio: modifica questo campo se per questo caso hai ricevuto indicatori antecedenti alla data di inizio inizialmente fornita. Valuta la possibilità di fornire ulteriori dettagli sull'indicatore appena rilevato nel campo della descrizione o di aggiungere un commento nella scheda Comunicazioni.

Comunicazioni

AWS I tecnici di Security Incident Response possono aggiungere commenti per documentare le loro attività quando lavorano su un caso. Diversi tecnici del AWS Security Incident Response possono lavorare su un caso contemporaneamente. Sono rappresentati come AWS Responder all'interno del registro delle comunicazioni.

Permissions

La scheda Autorizzazioni elenca tutte le persone che riceveranno una notifica in caso di modifica del caso. Puoi aggiungere e rimuovere persone dall'elenco fino alla chiusura del caso.

Note

I singoli casi consentono di includere fino a 30 parti interessate in totale. È necessaria una configurazione aggiuntiva delle autorizzazioni per concedere l'accesso a livello di caso a queste parti interessate.

Fornisci l'accesso a un caso nella console

Per fornire l'accesso al caso in Console di gestione AWS, puoi copiare il modello di policy di autorizzazione IAM e aggiungere questa autorizzazione a un utente o a un ruolo.

Aggiungere la policy IAM a un utente o a un ruolo:

1. Copia la politica di autorizzazione IAM.
2. Apri IAM in via <https://console.aws.amazon.com/iam/>.
3. Nel riquadro di navigazione, scegli Utente o Ruoli.
4. Seleziona un utente o un ruolo per aprire la pagina dei dettagli.
5. Nella scheda Autorizzazioni, scegli Aggiungi autorizzazioni.
6. Scegli Collega policy.
7. Seleziona la politica [AWS Security Incident Response gestita](#) appropriata.
8. Scegli Aggiungi policy.

Allegati

I soccorritori possono aggiungere allegati a un caso per aiutare gli altri soccorritori nelle indagini relative ai casi autogestiti.

Note

Se scegli un caso AWS supportato, non puoi visualizzare gli allegati AWS . Tutti i dettagli relativi ai casi AWS supportati devono essere condivisi tramite commenti sui casi o tramite la condivisione dello schermo da parte dell'utente utilizzando la tecnologia di comunicazione preferita.

Scegli Carica per selezionare un file dal tuo computer da aggiungere al caso.

Note

Tutti gli allegati caricati vengono eliminati sette giorni dopo la conclusione del caso. Closed

Tag

Un tag è un'etichetta opzionale che puoi assegnare ai tuoi casi per contenere i metadati relativi a quella risorsa. Ogni tag è un'etichetta composta da una chiave e un valore opzionale. Puoi utilizzare i tag per cercare, allocare i costi e autenticare le autorizzazioni per la risorsa.

Per aggiungere un tag, procedere come segue:

1. Scegli Aggiungi nuovo tag.
2. Per Chiave, inserisci il nome del tag.
3. In Valore, immetti il valore del tag.

Per rimuovere un tag, seleziona l'opzione Rimuovi per quel tag.

Attività relative ai casi

Gli audit trail forniscono registrazioni cronologiche dettagliate di tutte le attività del caso. Forniscono informazioni importanti sulle attività post-evento e aiutano a identificare potenziali miglioramenti. L'ora, l'utente, l'azione e i dettagli di ogni modifica del caso vengono registrati nell'audit trail del caso.

Chiusura di un caso

Per i casi AWS supportati, scegli Chiudi caso nella pagina dei dettagli del caso per chiudere definitivamente il caso in qualsiasi stato. Un caso raggiunge in genere lo stato Pronto a chiudere prima di essere chiuso definitivamente. Se si chiude prematuramente un caso in uno stato diverso da Pronto a chiudere, si richiede che i tecnici del AWS Security Incident Response smettano di lavorare su questo AWS caso supportato.

Se il tuo team di risposta agli incidenti è il responsabile della risposta, seleziona Azione/Chiudi caso nella pagina dei dettagli del caso.

Note

Lo stato «Pronto a chiudere» indica che un caso può essere chiuso definitivamente e che non è necessario eseguire ulteriori operazioni su un caso.

Una custodia non può essere riaperta dopo essere stata chiusa definitivamente. Tutte le informazioni saranno disponibili in sola lettura. Per evitare una chiusura accidentale, ti verrà chiesto di confermare che desideri chiudere la custodia.

Lavorare con CloudFormation StackSets

Important

AWS Security Incident Response non abilita le funzionalità di contenimento per impostazione predefinita. Per eseguire queste azioni di contenimento, è necessario concedere le autorizzazioni necessarie al servizio utilizzando i ruoli. AWS Identity and Access Management Puoi creare questi ruoli singolarmente per ogni account o per l'intera organizzazione distribuendo CloudFormation StackSets, StackSets Crea i ruoli richiesti.

Per istruzioni specifiche su come creare un account StackSet con autorizzazioni gestite dal servizio, consulta [Creazione con autorizzazioni gestite dal servizio nella CloudFormation StackSets Guida per l'utente](#).AWS CloudFormation

Di seguito sono riportati i modelli per creare i ruoli e.

AWSSecurityIncidentResponseContainmentAWSSecurityIncidentResponseContainmentExecution

```
AWSTemplateFormatVersion: '2010-09-09'
```

Description: 'Template for production SIR containment roles'

Resources:

AWSecurityIncidentResponseContainment:

Type: 'AWS::IAM::Role'

Properties:

RoleName: AWSecurityIncidentResponseContainment

AssumeRolePolicyDocument:

```
{
  'Version': '2012-10-17',
  'Statement':
  [
    {
      'Effect': 'Allow',
      'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
      'Action': 'sts:AssumeRole',
      'Condition': { 'StringEquals': { 'sts:ExternalId': !Sub
'${AWS::AccountId}' } } },
    },
    {
      'Effect': 'Allow',
      'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
      'Action': 'sts:TagSession',
    },
  ],
}
```

Policies:

- PolicyName: AWSecurityIncidentResponseContainmentPolicy

PolicyDocument:

```
{
  'Version': '2012-10-17',
  'Statement':
  [
    {
      'Effect': 'Allow',
      'Action': ['ssm:StartAutomationExecution'],
      'Resource':
      [
        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainEC2Instance:$DEFAULT',
        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainS3Resource:$DEFAULT',
        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainIAMPrincipal:$DEFAULT',
```

```

        ],
      },
    {
      'Effect': 'Allow',
      'Action':
        ['ssm:DescribeInstanceInformation', 'ssm:GetAutomationExecution',
'ssm:ListCommandInvocations'],
      'Resource': '*',
    },
  ],
  {
    'Effect': 'Allow',
    'Action': ['iam:PassRole'],
    'Resource': !GetAtt
AWSecurityIncidentResponseContainmentExecution.Arn,
    'Condition': { 'StringEquals': { 'iam:PassedToService':
'ssm.amazonaws.com' } } },
  },
],
}

AWSecurityIncidentResponseContainmentExecution:
  Type: 'AWS::IAM::Role'
  Properties:
    RoleName: AWSecurityIncidentResponseContainmentExecution
    AssumeRolePolicyDocument:
      {
        'Version': '2012-10-17',
        'Statement':
          [{ 'Effect': 'Allow', 'Principal': { 'Service': 'ssm.amazonaws.com' },
'Action': 'sts:AssumeRole' } ] },
      }
    ManagedPolicyArns:
      - !Sub arn:${AWS::Partition}:iam::aws:policy/SecurityAudit
    Policies:
      - PolicyName: AWSecurityIncidentResponseContainmentExecutionPolicy
        PolicyDocument:
          {
            'Version': '2012-10-17',
            'Statement':
              [
                {
                  'Sid': 'AllowIAMContainment',
                  'Effect': 'Allow',
                  'Action':
                    [

```

```
        'iam:AttachRolePolicy',
        'iam:AttachUserPolicy',
        'iam:DeactivateMFADevice',
        'iam>DeleteLoginProfile',
        'iam>DeleteRolePolicy',
        'iam>DeleteUserPolicy',
        'iam:GetLoginProfile',
        'iam:GetPolicy',
        'iam:GetRole',
        'iam:GetRolePolicy',
        'iam:GetUser',
        'iam:GetUserPolicy',
        'iam:ListAccessKeys',
        'iam:ListAttachedRolePolicies',
        'iam:ListAttachedUserPolicies',
        'iam:ListMfaDevices',
        'iam:ListPolicies',
        'iam:ListRolePolicies',
        'iam:ListUserPolicies',
        'iam:ListVirtualMFADevices',
        'iam:PutRolePolicy',
        'iam:PutUserPolicy',
        'iam:TagMFADevice',
        'iam:TagPolicy',
        'iam:TagRole',
        'iam:TagUser',
        'iam:UntagMFADevice',
        'iam:UntagPolicy',
        'iam:UntagRole',
        'iam:UntagUser',
        'iam:UpdateAccessKey',
        'identitystore:CreateGroupMembership',
        'identitystore>DeleteGroupMembership',
        'identitystore:IsMemberInGroups',
        'identitystore:ListUsers',
        'identitystore:ListGroups',
        'identitystore:ListGroupMemberships',
    ],
    'Resource': '*',
  },
  {
    'Sid': 'AllowOrgListAccounts',
    'Effect': 'Allow',
    'Action': 'organizations:ListAccounts',
```

```
        'Resource': '*',
    },
    {
        'Sid': 'AllowSSOContainment',
        'Effect': 'Allow',
        'Action':
            [
                'sso:CreateAccountAssignment',
                'sso:DeleteAccountAssignment',
                'sso:DeleteInlinePolicyFromPermissionSet',
                'sso:GetInlinePolicyForPermissionSet',
                'sso:ListAccountAssignments',
                'sso:ListInstances',
                'sso:ListPermissionSets',
                'sso:ListPermissionSetsProvisionedToAccount',
                'sso:PutInlinePolicyToPermissionSet',
                'sso:TagResource',
                'sso:UntagResource',
            ],
        'Resource': '*',
    },
    {
        'Sid': 'AllowSSORead',
        'Effect': 'Allow',
        'Action': ['sso-directory:SearchUsers', 'sso-
directory:DescribeUser'],
        'Resource': '*',
    },
    {
        'Sid': 'AllowS3Read',
        'Effect': 'Allow',
        'Action':
            [
                's3:GetAccountPublicAccessBlock',
                's3:GetBucketAcl',
                's3:GetBucketLocation',
                's3:GetBucketOwnershipControls',
                's3:GetBucketPolicy',
                's3:GetBucketPolicyStatus',
                's3:GetBucketPublicAccessBlock',
                's3:GetBucketTagging',
                's3:GetEncryptionConfiguration',
                's3:GetObject',
                's3:GetObjectAcl',
```

```

        's3:GetObjectTagging',
        's3:GetReplicationConfiguration',
        's3:ListBucket',
        's3express:GetBucketPolicy',
    ],
    'Resource': '*',
},
{
    'Sid': 'AllowS3Write',
    'Effect': 'Allow',
    'Action':
    [
        's3:CreateBucket',
        's3>DeleteBucketPolicy',
        's3>DeleteObjectTagging',
        's3:PutAccountPublicAccessBlock',
        's3:PutBucketACL',
        's3:PutBucketOwnershipControls',
        's3:PutBucketPolicy',
        's3:PutBucketPublicAccessBlock',
        's3:PutBucketTagging',
        's3:PutBucketVersioning',
        's3:PutObject',
        's3:PutObjectAcl',
        's3express:CreateSession',
        's3express>DeleteBucketPolicy',
        's3express:PutBucketPolicy',
    ],
    'Resource': '*',
},
{
    'Sid': 'AllowAutoScalingWrite',
    'Effect': 'Allow',
    'Action':
    [
        'autoscaling:CreateOrUpdateTags',
        'autoscaling>DeleteTags',
        'autoscaling:DescribeAutoScalingGroups',
        'autoscaling:DescribeAutoScalingInstances',
        'autoscaling:DescribeTags',
        'autoscaling:EnterStandby',
        'autoscaling:ExitStandby',
        'autoscaling:UpdateAutoScalingGroup',
    ],

```

```
    'Resource': '*',
  },
  {
    'Sid': 'AllowEC2Containment',
    'Effect': 'Allow',
    'Action': [
      'ec2:AuthorizeSecurityGroupEgress',
      'ec2:AuthorizeSecurityGroupIngress',
      'ec2:CopyImage',
      'ec2:CreateImage',
      'ec2:CreateSecurityGroup',
      'ec2:CreateSnapshot',
      'ec2:CreateTags',
      'ec2>DeleteSecurityGroup',
      'ec2>DeleteTags',
      'ec2:DescribeImages',
      'ec2:DescribeInstances',
      'ec2:DescribeSecurityGroups',
      'ec2:DescribeSnapshots',
      'ec2:DescribeTags',
      'ec2:ModifyNetworkInterfaceAttribute',
      'ec2:RevokeSecurityGroupEgress',
    ],
    'Resource': '*',
  },
  {
    'Sid': 'AllowKMSActions',
    'Effect': 'Allow',
    'Action': [
      'kms:CreateGrant',
      'kms:DescribeKey',
      'kms:GenerateDataKeyWithoutPlaintext',
      'kms:ReEncryptFrom',
      'kms:ReEncryptTo',
    ],
    'Resource': '*',
  },
  {
    'Sid': 'AllowSSMActions',
    'Effect': 'Allow',
    'Action': ['ssm:DescribeAutomationExecutions'],
    'Resource': '*',
  }
}
```

```
    },  
  ],  
}
```

Annulare l'iscrizione

Un ruolo che CancelMembership dispone dell'autorizzazione AWS Security Incident Response può annullare l'iscrizione dalla console, dall'API o AWS Command Line Interface.

Important

Una volta annullata l'iscrizione, non sarà possibile visualizzare i dati storici dei casi. Quando annulli un'iscrizione, la tua iscrizione verrà eliminata immediatamente e non avrai più accesso ai casi relativi all'iscrizione. Eventuali risorse o indagini che sono `Active` o `ready to close` verranno anch'esse sospese in seguito alla cancellazione dell'iscrizione.

Quando annulli un abbonamento:

La tua iscrizione verrà eliminata e non avrai più accesso ai casi relativi all'iscrizione.

Important

Se ti iscrivi nuovamente al servizio, verrà creata una nuova iscrizione e le risorse relative ai casi disponibili nell'abbonamento precedente saranno accessibili solo se le hai scaricate prima dell'annullamento.

Dopo l'annullamento dell'iscrizione, tutti i membri del team di risposta agli incidenti relativi all'iscrizione ricevono una notifica via e-mail.

Important

Se hai creato un'iscrizione utilizzando un account amministratore delegato e utilizzi l' AWS Organizations API per rimuovere la designazione di amministratore delegato dall'account, l'iscrizione verrà interrotta immediatamente.

Taggare le risorse AWS Security Incident Response

Un tag è un'etichetta di metadati che si assegna o che si assegna a AWS una risorsa. AWS Ciascun tag è formato da una chiave e da un valore, Per i tag assegnati da te, puoi definire la chiave e il valore. Ad esempio, potresti definire la chiave come stage e il valore di una risorsa come test.

I tag consentono di:

- Identifica e organizza le tue risorse. AWS Molti Servizi AWS supportano l'etichettatura, quindi puoi assegnare lo stesso tag a risorse di servizi diversi per indicare che le risorse sono correlate.
- Tieni traccia dei costi. AWS Attivi questi tag sulla AWS Billing dashboard. AWS utilizza i tag per classificare i costi e fornirti un rapporto mensile sull'allocazione dei costi. Per ulteriori informazioni, consulta [Utilizzare i tag di allocazione dei costi](#) nella [AWS Billing User Guide](#).
- Controlla l'accesso alle tue risorse. AWS Per ulteriori informazioni, consulta [Controllo degli accessi tramite tag](#) nella [Guida per l'utente di IAM](#).

Fai riferimento al [riferimento all'AWS Security Incident Response API per l'etichettatura](#).

Utilizzo AWS CloudShell per l'utilizzo con AWS Security Incident Response

AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da Console di gestione AWS. È possibile eseguire AWS CLI comandi AWS sui servizi (incluso AWS Security Incident Response) utilizzando la shell preferita (Bash o Z shell). PowerShell E puoi farlo senza dover scaricare o installare strumenti da riga di comando.

Si [avvia AWS CloudShell da Console di gestione AWS](#), e AWS le credenziali utilizzate per accedere alla console sono automaticamente disponibili in una nuova sessione di shell. Questa preautenticazione AWS CloudShell degli utenti consente di ignorare la configurazione delle credenziali quando si interagisce con AWS servizi come Security Incident Response utilizzando la AWS CLI versione 2 (preinstallata nell'ambiente di calcolo della shell).

Indice

- [Ottenere le autorizzazioni IAM per AWS CloudShell](#)
- [Interazione con Security Incident Response tramite AWS CloudShell](#)

Ottenere le autorizzazioni IAM per AWS CloudShell

Utilizzando le risorse di gestione degli accessi fornite da AWS Identity and Access Management, gli amministratori possono concedere le autorizzazioni agli utenti IAM in modo che possano accedere AWS CloudShell e utilizzare le funzionalità dell'ambiente.

Il modo più rapido per un amministratore di concedere l'accesso agli utenti è tramite una AWS policy gestita. Una [policy gestita da AWS](#) è una policy autonoma che viene creata e amministrata da AWS. La seguente policy AWS gestita per CloudShell può essere allegata alle identità IAM:

- `AWSCloudShellFullAccess`: concede l'autorizzazione all'uso AWS CloudShell con accesso completo a tutte le funzionalità.

Se desideri limitare l'ambito di azioni che un utente IAM può eseguire AWS CloudShell, puoi creare una policy personalizzata che utilizzi la policy `AWSCloudShellFullAccess` gestita come modello. Per ulteriori informazioni sulla limitazione delle azioni disponibili per gli utenti in CloudShell, consulta [Gestire AWS CloudShell l'accesso e l'utilizzo con le politiche IAM](#) nella Guida per l'AWS CloudShell utente.

Note

La tua identità IAM richiede anche una policy che conceda l'autorizzazione a effettuare chiamate a Security Incident Response.

Interazione con Security Incident Response tramite AWS CloudShell

Dopo l'avvio AWS CloudShell da Console di gestione AWS, è possibile iniziare immediatamente a interagire con Security Incident Response utilizzando l'interfaccia a riga di comando.

Note

Quando si utilizza AWS Command Line Interface in AWS CloudShell, non è necessario scaricare o installare risorse aggiuntive. Inoltre, poiché hai già eseguito l'autenticazione alla shell, non è necessario configurare le credenziali prima di effettuare chiamate.

Utilizzo AWS CloudShell e risposta agli incidenti di sicurezza

1. Da Console di gestione AWS, avvia CloudShell scegliendo le seguenti opzioni disponibili nella barra di navigazione:
 - Scegli l' CloudShell icona.
 - Inizia a digitare «cloudshell» nella casella di ricerca, quindi scegli l'opzione. CloudShell
2. Usa lo standard AWS Command Line Interface per interagire con AWS Security Incident Response. Per un riferimento completo dei comandi CLI disponibili, consulta il [AWS CLI Command Reference for AWS Security Incident Response](#).

Registrazione delle chiamate all'API AWS Security Incident Response utilizzando AWS CloudTrail

AWS Security Incident Response è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in Security Incident Response. CloudTrail acquisisce tutte le chiamate API per Security Incident Response come eventi. Le chiamate acquisite includono chiamate dalla console Security Incident Response e chiamate in codice alle operazioni dell'API Security Incident Response. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Security Incident Response. 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, è possibile determinare la richiesta effettuata a Security Incident Response, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

Per ulteriori informazioni CloudTrail, consulta la [Guida AWS CloudTrail per l'utente](#).

Informazioni sulla risposta agli incidenti di sicurezza in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività in Security Incident Response, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti in Account AWS. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Per un registro continuo degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi [CloudTrailLake](#).

CloudTrail sentieri

Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando il Console di gestione AWS sono multiregionali. È possibile creare un trail per una singola Regione o per più Regioni tramite AWS CLI. La creazione di un percorso multiregionale è consigliata in quanto consente di registrare l'intera attività del proprio Regioni AWS account. Se si crea un trail per una singola Regione, è possibile visualizzare solo gli eventi registrati nella Regione AWS del trail. Per ulteriori informazioni sui trail, consulta [Creating a trail for your Account AWS](#) e [Creating a trail for an organization](#) nella Guida per l'utente di AWS CloudTrail .

Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. [Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail](#) Per informazioni sui prezzi di Amazon S3, consulta [Prezzi di Amazon S3](#).

CloudTrail Archivi di dati sugli eventi di Lake

CloudTrail Lake ti consente di eseguire query basate su SQL sui tuoi eventi. CloudTrail [Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC](#). ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i [selettori di eventi avanzati](#). I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per ulteriori informazioni su CloudTrail Lake, consulta [Working with AWS CloudTrail Lake](#) nella Guida per l'utente.AWS CloudTrail

CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake comportano dei costi. Quando crei un datastore di eventi, scegli l'[opzione di prezzo](#) da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. [Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione Prezzi.AWS CloudTrail](#)

Tutte le azioni di Security Incident Response vengono registrate CloudTrail e documentate nel [AWS Security Incident Response API Reference](#). Ad esempio, le chiamate alle CreateMembership UpdateCase azioni CreateCase e generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#).

Informazioni sulle voci dei file di registro di Security Incident Response

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l' CreateCase azione.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA00000000000000000000:user",
    "arn": "arn:aws:sts::123412341234:assumed-role/Admin/user",
    "accountId": "123412341234",
    "accessKeyId": "*****",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA00000000000000000000",
        "arn": "arn:aws:iam::123412341234:role/Admin",
        "accountId": "123412341234",
        "userName": "Admin"
      },
      "attributes": {
        "creationDate": "2024-10-13T06:32:53Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2024-10-13T06:40:45Z",
  "eventSource": "security-ir.amazonaws.com",
  "eventName": "CreateCase",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "1.2.3.4",
  "userAgent": "aws-cli/2.17.23 md/awscrt#0.20.11 ua/2.0 os/macos#23.6.0 md/arch#x86_64 lang/python#3.11.9 md/pyimpl#CPython cfg/retry-mode#standard md/installer#exe md/prompt#off md/command#security-ir.create-case",
```

```
"requestParameters": {
  "impactedServices": [
    "Amazon GuardDuty"
  ],
  "impactedAccounts": [],
  "clientToken": "testToken112345679",
  "resolverType": "Self",
  "description": "****",
  "engagementType": "Investigation",
  "watchers": [
    {
      "email": "****",
      "name": "****",
      "jobTitle": "****"
    }
  ],
  "membershipId": "m-r1abcdabcd",
  "title": "****",
  "impactedAwsRegions": [
    {
      "region": "ap-southeast-1"
    }
  ],
  "reportedIncidentStartDate": 1711553521,
  "threatActorIpAddresses": [
    {
      "ipAddress": "****",
      "userAgent": "browser"
    }
  ]
},
"responseElements": {
  "caseId": "0000000001"
},
"requestID": "2db4b08d-94a9-457a-9474-5892e6c8191f",
"eventID": "b3fa3990-db82-43be-b120-c81262cc2f19",
"readOnly": false,
"resources": [
  {
    "accountId": "123412341234",
    "type": "AWS::SecurityResponder::Case",
    "ARN": "arn:aws:security-ir:us-east-1:123412341234:case/*"
  }
],
```

```
"eventType": "AwsApiCall",  
"managementEvent": true,  
"recipientAccountId": "123412341234",  
"eventCategory": "Management"  
}
```

Gestione AWS Security Incident Response degli account con AWS Organizations

AWS Security Incident Response è integrato con AWS Organizations. L'account di AWS Organizations gestione dell'organizzazione può designare un account come amministratore delegato di AWS Security Incident Response. Questa azione si abilita AWS Security Incident Response come servizio affidabile in AWS Organizations. Per informazioni su come vengono concesse queste autorizzazioni, vedere [Utilizzo AWS Organizations con altri AWS servizi](#).

Le seguenti sezioni illustreranno le varie attività che è possibile eseguire come account amministratore delegato di Security Incident Response.

Indice

- [Considerazioni e consigli per l'utilizzo con AWS Security Incident Response AWS Organizations](#)
- [Abilitare l'accesso affidabile per Gestione dell'account AWS](#)
- [Autorizzazioni necessarie per designare un account amministratore delegato di Security Incident Response](#)
- [Designazione di un amministratore delegato per AWS Security Incident Response](#)
- [Gestione dell'appartenenza alle unità organizzative \(OUs\) per AWS Security Incident Response](#)
- [Aggiungere membri a AWS Security Incident Response](#)
- [Rimozione di membri da AWS Security Incident Response](#)

Considerazioni e consigli per l'utilizzo con AWS Security Incident Response AWS Organizations

Le considerazioni e i consigli seguenti possono aiutarti a capire come funziona un account amministratore delegato di Security Incident Response in: AWS Security Incident Response

Account amministratore delegato per AWS Security Incident Response

È possibile designare un account membro come account amministratore delegato di Security Incident Response. Ad esempio, se si designa un account membro *111122223333* in *Europe (Ireland)*, non è possibile designare un altro account membro in *555555555555* *Canada (Central)*. È necessario utilizzare lo stesso account dell'account amministratore delegato di Security Incident Response in tutte le altre regioni.

L'account amministratore delegato di Security Incident Response è configurato in modo specifico.
Regione AWS

Si designa un account amministratore delegato di Security Incident Response in uno solo Regione AWS durante la configurazione iniziale. Sebbene la configurazione sia regionale, AWS Security Incident Response offre una copertura a livello aziendale per tutti i dispositivi supportati. Regioni AWS I risultati di sicurezza forniti da Amazon GuardDuty AWS Security Hub CSPM vengono acquisiti da tutti i servizi supportati e Regioni AWS i casi vengono gestiti centralmente nella regione in cui è stato attivato l'abbonamento. È necessario aggiungere l'account amministratore e gli account membro delegati di Security Incident Response. AWS Organizations

Non è consigliabile impostare l'account di gestione dell'organizzazione come account amministratore delegato di Security Incident Response.

L'account di gestione dell'organizzazione può essere l'account amministratore delegato di Security Incident Response. Tuttavia, le best practice AWS di sicurezza seguono il principio del privilegio minimo e non consigliano questa configurazione.

La rimozione di un account amministratore delegato di Security Incident Response da un abbonamento live annulla immediatamente l'abbonamento.

Se si rimuove un account amministratore delegato di Security Incident Response, vengono AWS Security Incident Response rimossi tutti gli account membro associati a tale account amministratore delegato di Security Incident Response. AWS Security Incident Response non sarà più abilitato per tutti gli account dei membri.

Abilitare l'accesso affidabile per Gestione dell'account AWS

L'abilitazione dell'accesso affidabile per AWS Security Incident Response consente all'amministratore delegato dell'account di gestione di modificare le informazioni e i metadati (ad esempio, i dettagli di contatto principali o alternativi) specifici di ciascun account membro in. AWS Organizations

Utilizzare la procedura seguente per abilitare l'accesso affidabile per AWS Security Incident Response nella propria organizzazione.

Autorizzazioni minime

Per eseguire queste attività, è necessario soddisfare i seguenti requisiti:

- È possibile eseguire questa operazione solo dall'account di gestione dell'organizzazione.

- L'organizzazione deve avere [tutte le caratteristiche abilitate](#).

Console

Per abilitare l'accesso affidabile per AWS Security Incident Response

1. Accedi alla [console AWS Organizations](#). È necessario accedere come utente IAM, assumere un ruolo IAM o accedere come utente root (non consigliato) nell'account di gestione dell'organizzazione.
2. Scegli Servizi nel riquadro di navigazione.
3. Scegli AWS Security Incident Response nell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di AWS Security Incident Response dialogo Abilita accesso affidabile per, digita enable per confermarlo, quindi scegli Abilita accesso affidabile.

API/CLI

Per abilitare l'accesso affidabile per Gestione dell'account AWS

Dopo aver eseguito il comando seguente, è possibile utilizzare le credenziali dell'account di gestione dell'organizzazione per richiamare le operazioni dell'API di gestione dell'account che utilizzano il `--accountId` parametro per fare riferimento agli account dei membri di un'organizzazione.

- AWS CLI: [enable-aws-service-access](#)

L'esempio seguente abilita l'accesso affidabile per AWS Security Incident Response l'organizzazione dell'account chiamante.

```
$ aws organizations enable-aws-service-access \
    --service-principal security-
ir.amazonaws.com
```

Se ha esito positivo, questo comando non produrrà alcun output.

Autorizzazioni necessarie per designare un account amministratore delegato di Security Incident Response

È possibile scegliere di configurare l' AWS Security Incident Response iscrizione utilizzando l'amministratore delegato per. AWS Organizations Per informazioni su come vengono concesse queste autorizzazioni, consulta [Utilizzo AWS Organizations con altri AWS servizi](#).

Note

AWS Security Incident Response abilita automaticamente la relazione AWS Organizations di fiducia quando si utilizza la console per la configurazione e la gestione. Se si utilizza il CLI/ SDK , è necessario abilitarlo manualmente utilizzando l'[API Enable AWSService Access](#) to `trustsecurity-ir.amazonaws.com`.

In qualità di AWS Organizations manager, prima di designare l'account amministratore delegato di Security Incident Response per l'organizzazione, verifica di poter eseguire le seguenti AWS Security Incident Response azioni: `security-ir:CreateMembership` e `security-ir:UpdateMembership` Queste azioni consentono di designare l'account amministratore delegato di Security Incident Response per l'organizzazione utilizzando. AWS Security Incident Response È inoltre necessario assicurarsi di avere il permesso di eseguire le AWS Organizations azioni che consentono di recuperare informazioni sulla propria organizzazione.

Per concedere queste autorizzazioni, includi la seguente dichiarazione in una policy AWS Identity and Access Management (IAM) per il tuo account:

```
{
  "Sid": "PermissionsForSIRAdmin",
  "Effect": "Allow",
  "Action": [
    "security-ir:CreateMembership",
    "security-ir:UpdateMembership",
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
```

```

        "organizations:ListAccounts"
    ],
    "Resource": "*"
}

```

Se desideri designare il tuo account di AWS Organizations gestione come account amministratore delegato di Security Incident Response, il tuo account richiederà anche l'azione IAM:

CreateServiceLinkedRole Controlla [Considerazioni e consigli per l'utilizzo con AWS Security Incident Response AWS Organizations](#) prima di procedere con l'aggiunta delle autorizzazioni.

Per continuare a designare il tuo account di AWS Organizations gestione come account amministratore delegato di Security Incident Response, aggiungi la seguente dichiarazione alla policy IAM e sostituiscila **111122223333** con l' Account AWS ID del tuo AWS Organizations account di gestione:

```

{
  "Sid": "PermissionsToEnableSecurityIncidentResponse"
  "Effect": "Allow",
  "Action": [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource": "arn:aws:iam::111122223333:role/aws-service-role/security-ir.amazonaws.com/AWSServiceRoleForSecurityIncidentResponse",
  "Condition": {
    "StringLike": {
      "iam:AWSServiceName": "security-ir.amazonaws.com"
    }
  }
}

```

Designazione di un amministratore delegato per AWS Security Incident Response

Questa sezione fornisce i passaggi per designare un amministratore delegato nell'organizzazione. AWS Security Incident Response

In qualità di manager dell' AWS organizzazione, assicurati di leggere attentamente come funziona un account amministratore delegato di Security Incident Response. [Considerazioni e raccomandazioni](#)

Prima di procedere, assicurati di averlo fatto. [Autorizzazioni necessarie per designare un account amministratore delegato di Security Incident Response](#)

Scegliete un metodo di accesso preferito per designare un account amministratore delegato di Security Incident Response per la vostra organizzazione. Solo un dirigente può eseguire questo passaggio.

Console

1. Aprire la console Security Incident Response all'indirizzo <https://console.aws.amazon.com/security-ir/>

Per accedere, utilizza le credenziali di gestione della tua AWS Organizations organizzazione.

2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione in cui desideri designare l'account amministratore delegato di Security Incident Response per la tua organizzazione.
3. Segui la procedura guidata di configurazione per creare la tua iscrizione, incluso l'account amministratore delegato.

API/CLI

- Esegui `CreateMembership` utilizzando le credenziali della direzione Account AWS dell'organizzazione.
 - In alternativa, è possibile utilizzare AWS Command Line Interface per eseguire questa operazione. Il AWS CLI comando seguente designa un account amministratore delegato di Security Incident Response. Di seguito sono riportate le opzioni di stringa disponibili per configurare l'iscrizione:

```
"stringstring",  
  
    {  
      "customerAccountId": "stringstring",  
      "membershipName": "stringstring",  
      "customerType": "Standalone",  
      "organizationMetadata": {  
        "organizationId": "string",  
        "managementAccountId":  
  
        "delegatedAdministrators": [  
          "stringstring"  
        ]  
      }  
    }
```

```

{
    },
    "membershipAccountsConfigurations":
        "autoEnableAllAccounts": true,
        "organizationalUnits": [
            "string"
        ]
    },
    "incidentResponseTeam": [
        {
            "name": "string",
            "jobTitle": "stringstring",
            "email": "stringstring"
        }
    ],
    "internalIdentifier": "string",
    "membershipId": "stringstring",
    "optInFeatures": [
        {
            "featureName": "RuleForwarding",
            "isEnabled": true
        }
    ]
}

```

Se non AWS Security Incident Response è abilitato per l'account amministratore delegato di Security Incident Response, non sarà in grado di intraprendere alcuna azione. Se non l'hai già fatto, assicurati di attivarlo AWS Security Incident Response per l'account amministratore delegato di Security Incident Response appena designato.

Gestione dell'appartenenza alle unità organizzative (OUs) per AWS Security Incident Response

AWS Security Incident Response supporta la copertura associativa per le singole unità organizzative (OUs). Puoi aggiornare la tua iscrizione in base a una copertura specifica OUs in qualsiasi momento. Tutti gli account selezionati OUs, compresi gli account per minori OUs, saranno coperti dall'iscrizione.

Quando si aggiorna l'associazione di appartenenza, è possibile richiedere l'aggiornamento per un massimo di 5 membri OUs alla volta. Se desideri apportare modifiche a più di 5 OUs, completa le modifiche all'associazione in batch da 5 OUs fino al completamento di tutti gli aggiornamenti.

Console

1. Apri la console Security Incident Response all'indirizzo <https://console.aws.amazon.com/security-ir/>

Per accedere, utilizza le credenziali di gestione della tua AWS Organizations organizzazione.

2. Vai a Gestisci l'iscrizione > Account
3. Fai clic su Aggiorna associazione
4. Seleziona Scegli unità organizzative (OUs)
5. Seleziona Aggiungi OUs o rimuovi OUs
6. Seleziona fino a 5 OUs che desideri aggiornare. Non puoi aggiungere e rimuovere OUs contemporaneamente.

Note

Verranno associati tutti gli account e i figli OUs appartenenti a un'unità organizzativa selezionata.

7. Fai clic su Aggiorna associazione

8.

Note

Se desideri apportare modifiche a più di 5 OUs, ripeti i passaggi 5 e 6 fino a quando non saranno OUs stati associati tutti.

Per ulteriori informazioni su come apportare modifiche alle unità organizzative all'interno AWS dell'organizzazione, consulta [Gestire le unità organizzative \(OUs\) con AWS Organizations](#).

Aggiungere membri a AWS Security Incident Response

Esiste una relazione uno a uno con AWS Organizations e la tua AWS Security Incident Response iscrizione. Man mano che gli account vengono aggiunti (o rimossi) dalle tue Organizations o dalle tue unità organizzative (OUs), queste modifiche si rifletteranno negli account coperti dalla tua AWS Security Incident Response iscrizione.

Per aggiungere un account alla tua iscrizione, segui una delle opzioni per [Gestire gli account in un'organizzazione con AWS Organizations](#).

Puoi anche aggiungere altri membri OUs alla tua iscrizione in qualsiasi momento, vedi [Gestire l'appartenenza con le unità organizzative \(OUs\)](#).

Rimozione di membri da AWS Security Incident Response

Per rimuovere un account dalla tua iscrizione, puoi rimuovere un account membro dalla tua organizzazione, spostare gli account da quelli selezionati OUs o rimuoverlo OUs dall'iscrizione.

Per rimuovere un account dalla tua iscrizione, segui le procedure per [rimuovere un account membro da un'organizzazione](#).

Per trasferire gli account al di fuori del tuo OUs, segui le procedure relative [allo spostamento degli account in un'unità organizzativa \(OU\) o tra l'unità principale e OUs con AWS Organizations](#).

Per rimuovere l'unità organizzativa dalla tua iscrizione, segui le procedure per la [gestione dell'appartenenza alle unità organizzative \(OUs\)](#).

Amazon EventBridge

Con Amazon EventBridge, puoi reagire, monitorare e orchestrare gli eventi associati ai AWS Security Incident Response casi e alle iscrizioni. Puoi indirizzare questi eventi tramite Rules (per scenari fan-out verso uno o più obiettivi) o tramite Pipes (per point-to-point integrazioni con funzionalità avanzate di filtraggio, arricchimento e trasformazione).

Puoi creare integrazioni tra Security Incident Response e strumenti di terze parti o aggregare dati da analizzare utilizzando l'intelligenza artificiale generativa e altri strumenti. AWS Ad esempio, quando Security Incident Response crea un caso in modo proattivo, puoi utilizzare EventBridge le automazioni per attivare i sistemi di notifica alle parti interessate. Inoltre, se gestisci più AWS ambienti, puoi utilizzare l' EventBridge integrazione Amazon per monitorare le AWS Security Incident Response iscrizioni e garantire che tutti gli ambienti mantengano un elevato livello di sicurezza.

Per ulteriori informazioni puoi consultare la pagina [What is Amazon EventBridge?](#)

Note

Per gli ultimi aggiornamenti sull' EventBridge integrazione di Amazon con AWS Security Incident Response, incluse le integrazioni ITSM, consulta [AWS Security Incident Response ora supporta le integrazioni ITSM](#) nella pagina AWS What's New.

Indice

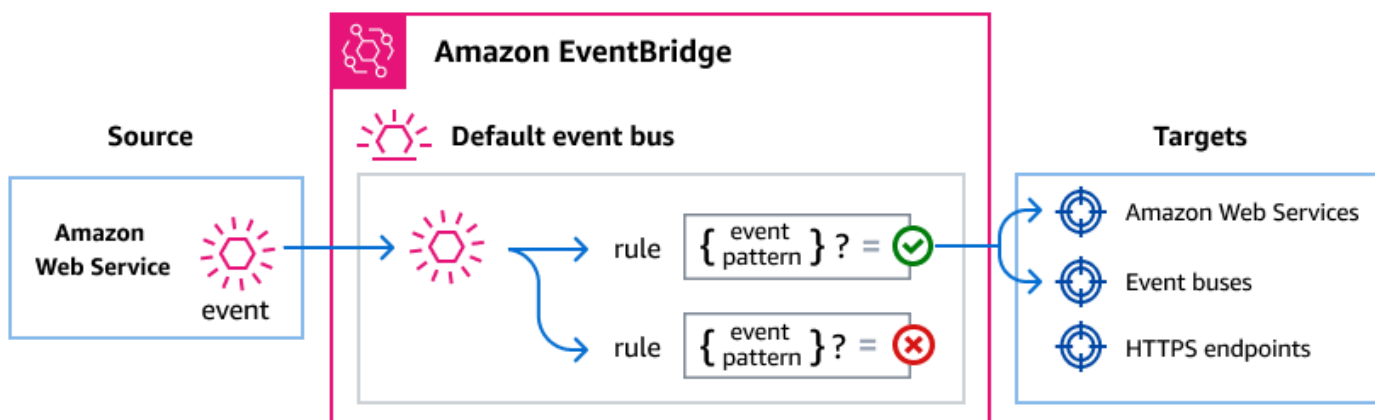
- [Gestione degli eventi di Security Incident Response tramite Amazon EventBridge](#)
- [Utilizzo AWS Security Incident Response degli eventi](#)
- [Tutorial: invio di avvisi Amazon Simple Notification Service per Membership Updated eventi](#)

Gestione degli eventi di Security Incident Response tramite Amazon EventBridge

Amazon EventBridge è un servizio serverless che utilizza gli eventi per connettere tra loro i componenti delle applicazioni, semplificando la creazione di applicazioni scalabili basate sugli eventi. L'architettura basata sugli eventi è uno stile di creazione di sistemi software ad accoppiamento debole che interagiscono emettendo e rispondendo agli eventi. Gli eventi rappresentano un cambiamento in una risorsa o in un ambiente.

Come funziona:

Come molti AWS servizi, Security Incident Response genera e invia eventi al bus di eventi predefinito. EventBridge (Il bus degli eventi predefinito viene fornito automaticamente nel tuo AWS account.) Un router di eventi è un router che riceve eventi e li invia a zero o più destinazioni o target. Le regole associate al router di eventi valutano questi ultimi man mano che arrivano. Ogni regola verifica se un evento corrisponde al modello della regola. Se l'evento corrisponde, il router di eventi invia l'evento al/ai target specificato/i.



Distribuzione di eventi Security Incident Response utilizzando EventBridge le regole

Per fare in modo che il bus degli eventi EventBridge predefinito invii gli eventi di Security Incident Response a una destinazione, è necessario creare una regola. Ogni regola contiene uno schema di eventi, che EventBridge corrisponde a ogni evento ricevuto sull'event bus. Se i dati dell'evento corrispondono al modello di evento specificato, EventBridge invia quell'evento ai destinatari della regola.

Per istruzioni complete sulla creazione di regole per i bus degli eventi, consulta [la sezione Creazione di regole che reagiscono agli eventi](#) nella Amazon EventBridge User Guide.

Creazione di pattern di eventi che corrispondano agli eventi di Security Incident Response

Ogni modello di eventi è un oggetto in formato JSON che contiene:

- Un attributo `source` che identifica il servizio che invia l'evento. Per gli eventi Security Incident Response, la fonte è `"aws.security-ir"`.

- (Facoltativo): Un attributo `detail-type` che contiene una serie di tipi di eventi da abbinare.
- (Facoltativo): Un attributo `detail` contenente qualsiasi altro dato relativo all'evento da abbinare.

Ad esempio, il seguente schema di eventi corrisponde a tutti Case Updated by AWS Security Incident Response Service gli eventi di un determinato periodo Account AWS:

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T03:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

Per ulteriori informazioni sulla scrittura di modelli di eventi, consultate [Event pattern](#) nella Guida EventBridge per l'utente.

Riferimento dettagliato agli eventi di Security Incident Response

Tutti gli eventi generati dai AWS servizi dispongono di un set comune di campi contenenti metadati relativi all'evento, ad esempio il AWS servizio da cui è generato l'evento, l'ora in cui l'evento è stato generato, l'account e la regione in cui si è verificato l'evento e altri. Per le definizioni di questi campi generali, consulta il [riferimento alla struttura degli eventi](#) nella Amazon EventBridge User Guide.

Inoltre, ogni evento ha un campo `detail` che contiene dati specifici per quel particolare evento. Il riferimento seguente definisce i campi di dettaglio per i vari eventi di Security Incident Response.

Quando si utilizza EventBridge per selezionare e gestire gli eventi di Security Incident Response, è utile tenere presente quanto segue:

- Il `source` campo per tutti gli eventi di Security Incident Response è impostato su `"aws.security-ir"`.
- Il campo `detail-type` specifica il tipo di evento.

Ad esempio, `"Case Updated"`.

- Il campo `detail` contiene i dati specifici di quel particolare evento.

Per informazioni sulla creazione di modelli di eventi che consentono alle regole di corrispondere agli eventi di Security Incident Response, consulta [Event pattern](#) nella Amazon EventBridge User Guide.

Per ulteriori informazioni sugli eventi e su come li EventBridge elabora, consulta [EventBridge gli eventi](#) nella Amazon EventBridge User Guide.

Campi comuni: tutti AWS Security Incident Response gli eventi includono questi EventBridge campi Amazon standard

- `versione`: versione in formato EventBridge evento
- `id`: identificatore univoco dell'evento
- `detail-type`: descrizione leggibile dall'uomo del tipo di evento
- `fonte`: sempre «aws.security-ir» per gli eventi di Security Incident Response
- `account`: ID dell'account in cui si è AWS verificato l'evento
- `ora`: timestamp ISO 8601 in cui si è verificato l'evento
- `regione`: Regione AWS dove esiste la risorsa
- `risorse`: Array contenente l'ARN della risorsa interessata

Campi di dettaglio: l'`detail` oggetto contiene informazioni specifiche sulla risposta agli incidenti di sicurezza

- `CaseID`: identificatore univoco per il caso (solo eventi relativi al caso)
- `MembershipID`: identificatore univoco per l'iscrizione (solo eventi di iscrizione)
- `UpdateBy`: chi ha eseguito l'aggiornamento (solo eventi di aggiornamento di maiuscole e commenti)
- `CreatedBy`: chi ha creato l'entità (solo eventi di creazione di casi e commenti)

Valori degli attori: i `createdBy` campi `updatedBy` and possono contenere

- AWS Risponditore: azione eseguita da un addetto AWS alla sicurezza
- *security-ir.amazonaws.com*: Azione eseguita automaticamente dal servizio
- ID account: azione eseguita dal cliente (ad esempio, «111122223333»)

Valori ARN delle risorse: AWS Security Incident Response le risorse utilizzano questi formati ARN

- Casi: `arn:aws:security-ir:{region}:{account-id}:case/{case-id}`
- Abbonamenti: `arn:aws:security-ir:{region}:{account-id}:membership/{membership-id}`

Eventi del caso

Caso creato da AWS Responder

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "AWS Responder"
  }
}
```

Caso creato dal servizio

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
```

```
"source": "aws.security-ir",
"account": "111122223333",
"time": "2023-05-12T00:00:00Z",
"region": "us-west-2",
"resources": [
  "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
],
"detail": {
  "caseId": "1234567890",
  "createdBy": "security-ir.amazonaws.com"
}
}
```

Caso creato dal cliente

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "111122223333"
  }
}
```

Caso aggiornato dal AWS risponditore

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
```

```
"account": "111122223333",
"time": "2023-05-12T01:30:00Z",
"region": "us-west-2",
"resources": [
  "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
],
"detail": {
  "caseId": "1234567890",
  "updatedBy": "AWS Responder"
}
}
```

Caso aggiornato dal cliente AWS

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "111122223333"
  }
}
```

Caso aggiornato dal AWS Security Incident Response servizio

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
```

```
    "time": "2023-05-12T03:45:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "updatedBy": "security-ir.amazonaws.com"
    }
  }
}
```

Caso chiuso

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Closed",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-15T14:22:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890"
  }
}
```

Eventi relativi ai commenti sul caso

Commento al caso creato da AWS Responder

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
```

```

    "time": "2023-05-12T04:30:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "createdBy": "AWS Responder"
    }
  }
}

```

Commento al caso creato dal cliente

```

{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "111122223333"
  }
}

```

Commento al caso creato dal AWS Security Incident Response servizio

```

{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",

```

```
"region": "us-west-2",
"resources": [
  "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
],
"detail": {
  "caseId": "1234567890",
  "createdBy": "security-ir.amazonaws.com"
}
}
```

Commento al caso aggiornato dal cliente

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "111122223333"
  }
}
```

Commento al caso aggiornato dal AWS Security Incident Response servizio

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
```

```
"resources": [  
  "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"  
],  
"detail": {  
  "caseId": "1234567890",  
  "updatedBy": "security-ir.amazonaws.com"  
}  
}
```

Commento al caso creato da AWS Responder

```
{  
  "version": "0",  
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",  
  "detail-type": "Case Comment Updated",  
  "source": "aws.security-ir",  
  "account": "111122223333",  
  "time": "2023-05-12T02:45:00Z",  
  "region": "us-west-2",  
  "resources": [  
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"  
  ],  
  "detail": {  
    "caseId": "1234567890",  
    "updatedBy": "AWS Responder"  
  }  
}
```

Eventi per i soci

Iscrizione creata

```
{  
  "version": "0",  
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",  
  "detail-type": "Membership Created",  
  "source": "aws.security-ir",  
  "account": "111122223333",  
  "time": "2023-04-01T10:00:00Z",
```

```

    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
    ],
    "detail": {
      "membershipId": "m-1234567890abcdef0"
    }
  }
}

```

Iscrizione aggiornata

```

{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Membership Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-04-15T16:30:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
  ],
  "detail": {
    "membershipId": "m-1234567890abcdef0"
  }
}

```

Iscrizione annullata

```

{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Membership Closed",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-06-30T23:59:59Z",
  "region": "us-west-2",

```

```

    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
    ],
    "detail": {
      "membershipId": "m-1234567890abcdef0"
    }
  }

```

Iscrizione terminata

```

{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Membership Terminated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-07-01T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:membership/
m-123456s7890abcdef0"
  ],
  "detail": {
    "membershipId": "m-1234567890abcdef0"
  }
}

```

Utilizzo AWS Security Incident Response degli eventi

Puoi creare EventBridge regole per abbinare questi eventi e attivare azioni automatiche. Di seguito sono riportati alcuni esempi di casi d'uso:

Abbina tutti AWS Security Incident Response gli eventi:

```

{
  "source": ["aws.security-ir"]
}

```

Corrisponde solo agli eventi casuali:

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
    "Case Comment Added",
    "Case Comment Updated"
  ]
}
```

Corrispondi ai casi aggiornati dai AWS risponditori:

```
{
  "source": ["aws.security-ir"],
  "detail-type": ["Case Updated"],
  "detail": {
    "updatedBy": ["AWS Responder"]
  }
}
```

Abbina gli eventi per un caso specifico:

```
{
  "source": ["aws.security-ir"],
  "detail": {
    "caseId": ["1234567890"]
  }
}
```

Tutorial: invio di avvisi Amazon Simple Notification Service per **Membership Updated** eventi

In questo tutorial, configuri una regola EventBridge degli eventi Amazon che acquisisce solo gli eventi in cui l'abbonamento entra in uno **Membership Updated** stato.

Prerequisiti

Questo tutorial presuppone che tu abbia un abbonamento funzionante e AWS account attivi nel tuo abbonamento.

Argomenti

- [Tutorial: creare e sottoscrivere un argomento di Amazon SNS](#)
- [Tutorial: Registra una regola di evento](#)
- [Tutorial: verifica la tua regola](#)
- [Regola alternativa: Security Incident Response Case Updates](#)

Tutorial: creare e sottoscrivere un argomento di Amazon SNS

In questo tutorial, configuri un argomento Amazon SNS che funga da destinazione evento per la nuova regola di evento.

Come creare un argomento Amazon SNS

1. [Apri la console Amazon SNS nella versione v3/home. https://console.aws.amazon.com/sns/](https://console.aws.amazon.com/sns/)
2. Scegliere Topics (Argomenti), Create topic (Crea argomento).
3. Per Tipo, scegliere Standard.
4. Per Nome, inserisci **MembershipUpdated** e scegli Crea argomento.
5. Sullo MembershipUpdated schermo, scegli Crea abbonamento.
6. Per Protocollo, scegli E-mail.
7. In Endpoint, inserire un indirizzo e-mail a cui si ha accesso correntemente, quindi scegliere Crea sottoscrizione.
8. Controlla l'account e-mail e attendi di ricevere una e-mail di conferma della sottoscrizione. Una volta ricevuta, seleziona Confirm subscription (Conferma sottoscrizione).

Tutorial: Registra una regola di evento

Quindi, registra una regola di evento che catturi solo Membership Updated gli eventi.

Per registrare la tua regola EventBridge

1. Apri la EventBridge console Amazon all'indirizzo <https://console.aws.amazon.com/events/>.
2. Nel pannello di navigazione, scegli Regole.
3. Scegli Crea regola.
4. Inserisci un nome e una descrizione per la regola.

Note

Una regola non può avere lo stesso nome di un'altra regola nella stessa Regione e sullo stesso router di eventi.

5. Per Select event bus (Seleziona bus di eventi), scegli il bus di eventi che desideri associare a questa regola. Se la regola deve cercare eventi corrispondenti provenienti dal tuo account, seleziona Bus di eventi predefiniti di AWS . Quando un AWS servizio del tuo account emette un evento, questo passa sempre al bus eventi predefinito del tuo account.

Note

Questo deve essere configurato nel tuo account amministratore delegato AWS Organizations o nel quale hai creato l' AWS Security Incident Response iscrizione.

6. Per Tipo di regola, scegli Regola con un modello di eventi.
7. Scegli Next (Successivo).
8. In Event source (Origine eventi), scegli Other (Altro).
9. Per Event pattern, seleziona Modelli personalizzati (editor JSON).
10. Incolla il modello di eventi seguente nell'area di testo.

```
{
  "source": ["aws.security-ir"],
  "detail-type": ["Membership Updated"]
}
```

Questo codice definisce una EventBridge regola che corrisponde a qualsiasi evento in cui l'iscrizione al servizio viene aggiornata o modificata. Per ulteriori informazioni sui pattern di eventi, consulta [Events and Event Patterns](#) nella Amazon EventBridge User Guide.

11. Scegli Next (Successivo).
12. Per Tipi di destinazione, scegli servizio AWS .
13. Per Seleziona un target, scegli l'argomento SNS e per Argomento, scegli MembershipUpdated.
14. (Facoltativo) Per Additional settings (Impostazioni aggiuntive), procedi come segue:
 - a. Per Maximum age of event (Età massima dell'evento), immetti un valore compreso tra un minuto (00:01) e 24 ore (24:00).
 - b. Per Tentativi, specifica un numero compreso tra 0 e 185.
 - c. Per la coda di lettere non scritte, scegli se utilizzare una coda Amazon SQS standard come coda di lettere non scritte. EventBridge invia gli eventi che corrispondono a questa regola alla coda di lettere non scritte se non vengono consegnati correttamente alla destinazione. Esegui una delle seguenti operazioni:
 - Scegli Nessuna per non utilizzare una coda DLQ.
 - Scegli Seleziona una coda Amazon SQS nell' AWS account corrente da utilizzare come coda di lettere non scritte, quindi seleziona la coda da utilizzare dal menu a discesa.
 - Scegli Seleziona una coda Amazon SQS in un altro AWS account come coda di lettere non scritte, quindi inserisci l'ARN della coda da utilizzare. È necessario allegare una policy basata sulle risorse alla coda che conceda l'autorizzazione a inviarle messaggi. EventBridge Per ulteriori informazioni, consulta [Concessione delle autorizzazioni alla coda delle lettere non scritte nella Amazon](#) User Guide. EventBridge
15. Scegli Next (Successivo).
16. (Facoltativo) Inserire uno o più tag per la regola. Per ulteriori informazioni, consulta i [EventBridge tag Amazon](#) nella Amazon EventBridge User Guide.
17. Scegli Next (Successivo).
18. Rivedi i dettagli della regola e scegli Crea regola.

Tutorial: verifica la tua regola

Per verificare la tua regola, invia un aggiornamento della tua AWS Security Incident Response iscrizione. Se la regola è configurata correttamente, riceverai entro pochi minuti un messaggio e-mail con il testo dell'evento.

Regola alternativa: Security Incident Response Case Updates

Per creare una regola degli eventi che monitora tutti gli aggiornamenti dei casi, ripeti questi tutorial con le seguenti modifiche:

1. In [Tutorial: creare e sottoscrivere un argomento di Amazon SNS](#), usa *CaseUpdates* come nome dell'argomento.
2. In [Tutorial: Registra una regola di evento](#), usa il seguente schema nell'editor JSON:

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
    "Case Comment Created",
    "Case Comment Updated"
  ]
}
```

Risoluzione dei problemi

In caso di problemi relativi all'esecuzione di un'azione specifica per AWS Security Incident Response, consulta gli argomenti di questa sezione.

Un ERRORE è uno stato di un'operazione che denota un errore in alcune o tutte le operazioni. In alternativa, si ricevono avvisi quando si verifica un problema ma l'attività viene comunque completata.

Indice

- [Problemi](#)
- [Errori](#)
- [Supporto](#)

Problemi

Non invio di richieste dal contesto corretto.

Tutte le chiamate a AWS Security Incident Response APIs devono provenire da un principale IAM nell'account di amministratore delegato del servizio o dell'account di iscrizione. Assicurati di operare con il principale IAM corretto, Account AWS ovvero l'account di amministratore AWS Security Incident Response delegato o di iscrizione della tua organizzazione.

Errori

`AccessDeniedException`

Non disponi dell'autorizzazione di accesso sufficiente per eseguire questa operazione.

Collabora con il tuo AWS amministratore per assicurarti di avere l'autorizzazione ad assumere un ruolo IAM nel tuo account di amministratore AWS Security Incident Response delegato o di iscrizione. Verifica anche che il ruolo abbia una policy IAM che consenta l'azione richiesta. Per ulteriori informazioni, consulta [AWS Security Incident Response IAM](#).

`ConflictException`

La richiesta causa uno stato incoerente.

Verifica che tutti i nomi dei file allegati o i membri del team di risposta predefiniti che hai specificato siano univoci. Verifica inoltre che l'iscrizione AWS Security Incident Response al servizio

non sia già stata configurata. Apri la console Security Incident Response all'indirizzo <https://console.aws.amazon.com/security-ir/> e accedi a [Membership Details](#).

InternalServerErrorException

Si è verificato un errore imprevisto durante l'elaborazione della richiesta. Riprova tra qualche minuto. Se il problema persiste, [solleva un caso con Supporto](#).

ResourceNotFoundException

La richiesta fa riferimento a una risorsa che non esiste.

Una o più risorse specificate nella richiesta non esistono. Verifica che tutte le risorse fornite IDs siano ARNs corrette. Ciò si applica all'account AWS Organizations IDs, ai ruoli IAM IDs, alle appartenenze, ai casi, ai membri del team di risposta, ai casi, ai responsabili delle risposte ai casi, agli allegati dei casi e ai commenti dei casi.

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Il responsabile IAM ha fatto troppe richieste a quella funzione API in un determinato periodo. Attendi un minuto e riprova. Se il problema persiste, prendi in considerazione l'implementazione di un algoritmo esponenziale di backoff e riprova.

ValidationException

L'input non soddisfa i vincoli specificati da un Servizio AWS

Uno o più campi dati della richiesta non soddisfano i requisiti di combinazione and/or logica di convalida. Verifica che tutte le risorse siano ARNs complete e che i valori di testo soddisfino i vincoli di dimensione e formato indicati nella Guida di riferimento delle [AWS Security Incident Response API](#). Verifica inoltre che siano consentiti eventuali aggiornamenti dei valori. Ad esempio, non è possibile modificare un caso da AWS supportato a autogestito.

Supporto

Se hai bisogno di ulteriore assistenza, contatta il [Supporto Centro](#) per la risoluzione dei problemi. Tieni a disposizione le seguenti informazioni:

- Quello Regione AWS che hai usato

- L' Account AWS ID dell'iscrizione
- Il contenuto di origine, se applicabile e disponibile
- Eventuali altri dettagli sul problema che potrebbero essere utili per la risoluzione dei problemi

Sicurezza

Indice

- [Protezione dei dati in AWS Security Incident Response](#)
- [Riservatezza del traffico inter-rete](#)
- [Identity and Access Management](#)
- [Risoluzione dei problemi di AWS Security Incident Response identità e accesso](#)
- [Utilizzo dei ruoli di servizio](#)
- [Uso di ruoli collegati ai servizi](#)
- [AWS Policy gestite](#)
- [Risposta agli incidenti](#)
- [Convalida della conformità](#)
- [Registrazione e monitoraggio in AWS Security Incident Response](#)
- [Resilienza](#)
- [Sicurezza dell'infrastruttura](#)
- [Analisi della configurazione e delle vulnerabilità](#)
- [Prevenzione del problema "confused deputy" tra servizi](#)

Protezione dei dati in AWS Security Incident Response

Indice

- [Crittografia dei dati](#)

Il [modello di responsabilità AWS condivisa](#) si applica alla protezione dei dati per il servizio AWS Security Incident Response. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura che gestisce i servizi offerti nel AWS Cloud. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile delle attività di configurazione e gestione della sicurezza per i AWS servizi che utilizza. Per ulteriori informazioni sulla privacy dei dati, consulta [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post [AWS Modello di responsabilità condivisa](#) e GDPRAWS nel blog sulla sicurezza di .

Ai fini della protezione dei dati, le best practice di AWS sicurezza stabiliscono che è necessario proteggere le credenziali AWS dell'account e configurare i singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In questo modo, a ciascun utente vengono concesse solo le autorizzazioni necessarie per adempiere alle proprie mansioni lavorative. Sugeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS dei servizi.
- FIPS 140-3 non è attualmente supportato dal servizio.

Non dovresti mai inserire informazioni riservate o sensibili, come i tuoi indirizzi e-mail, in tag o campi di testo in formato libero come il campo Nome. Ciò include quando lavori con AWS Support o altri AWS servizi utilizzando la console, l'API, la AWS CLI o AWS SDKs. Tutti i dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i registri di fatturazione o diagnostica. Se fornisci un URL a un server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali nell'URL per convalidare la tua richiesta a quel server.

Crittografia dei dati

Indice

- [Crittografia dei dati a riposo](#)
- [Crittografia dei dati in transito](#)
- [Gestione delle chiavi](#)

Crittografia dei dati a riposo

I dati vengono crittografati a riposo utilizzando la crittografia lato server trasparente. Questo consente di ridurre gli oneri operativi e la complessità associati alla protezione dei dati sensibili. La crittografia dei dati inattivi consente di creare applicazioni sicure che rispettano rigorosi requisiti normativi e di conformità per la crittografia.

Crittografia dei dati in transito

I dati raccolti e a cui accede AWS Security Incident Response avvengono esclusivamente su un canale protetto Transport Layer Security (TLS).

Gestione delle chiavi

AWS Security Incident Response implementa integrazioni AWS KMS per fornire la crittografia a riposo dei dati relativi ai casi e agli allegati.

AWS Security Incident Response non supporta le chiavi gestite dal cliente.

Riservatezza del traffico inter-rete

Traffico tra servizio e applicazioni e client locali

Sono disponibili due opzioni di connettività tra la rete privata e AWS:

- Una AWS Site-to-Site VPN connessione. Per ulteriori informazioni, consulta [Che cos'è AWS Site-to-Site VPN?](#) nella Guida per l'utente di AWS Site-to-Site VPN .
- Una Direct Connect connessione. Per ulteriori informazioni, consulta [Che cos'è Direct Connect?](#) nella Guida per l'utente di Direct Connect .

L'accesso AWS Security Incident Response tramite la rete avviene tramite AWS published APIs. I client devono supportare Transport Layer Security (TLS) 1.2. È consigliabile TLS 1.3. I client devono inoltre supportare le suite di cifratura con PFS (Perfect Forward Secrecy), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). La maggior parte dei sistemi moderni come Java 7 e versioni successive, supporta tali modalità. Inoltre, è necessario firmare le richieste utilizzando un ID chiave di accesso e la chiave di accesso segreta associate a un principale IAM, oppure è possibile utilizzare [AWS Security Token Service \(STS\)](#) per generare le credenziali di sicurezza temporanee per firmare le richieste.

Traffico tra AWS risorse nella stessa regione

Un endpoint Amazon Virtual Private Cloud (Amazon VPC) per AWS Security Incident Response è un'entità logica all'interno di un VPC che consente la connettività solo a. AWS Security Incident Response Amazon VPC indirizza le richieste AWS Security Incident Response e le risposte al VPC. Per ulteriori informazioni, consultare [Endpoint VPC](#) nella Guida per l'utente di Amazon VPC. Per le

policy di esempio che possono essere utilizzate per controllare l'accesso da endpoint VPC, consulta [Utilizzo delle policy IAM per controllare l'accesso a DynamoDB](#).

Note

Gli endpoint Amazon VPC non sono accessibili tramite o. AWS Site-to-Site VPN Direct Connect

Identity and Access Management

AWS Identity and Access Management (IAM) è AWS un servizio che aiuta un amministratore a controllare l'accesso AWS alle risorse. Gli amministratori IAM controllano i principali autenticati (connessi) e autorizzati (dispongono delle autorizzazioni) per l'utilizzo delle risorse. AWS Security Incident Response IAM è un AWS servizio che puoi utilizzare senza costi aggiuntivi.

Indice

- [Autenticazione con identità](#)
- [Come AWS Security Incident Response funziona con IAM](#)

Pubblico

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro che AWS Security Incident Response svolgi.

Amministratori della sicurezza

Si consiglia a questi utenti di utilizzare la policy [AWSSecurityIncidentResponseFullAccess](#) gestita per assicurarsi di avere accesso in lettura e scrittura alle risorse relative ai membri e ai casi.

Case Watchers

Queste persone non hanno accesso autorevole a tutti i casi, ma a singoli casi per i quali concedi un'autorizzazione esplicita.

Membri dell'Incident Response Team

Ai membri del team può essere concessa sia l'iscrizione completa che l'accesso ai casi. Si raccomanda che non tutte le persone intraprendano azioni autorevoli in merito all'iscrizione al

servizio, ma dovrebbero avere accesso a tutti i casi creati e gestiti tramite il servizio. Per ulteriori informazioni, consulta le politiche [AWS Security Incident Response gestite](#).

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. È necessario autenticarsi (accedere a AWS) come utente root dell' AWS account, come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS Gli utenti di IAM Identity Center (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere alla Console di AWS gestione o al portale di AWS accesso. Per ulteriori informazioni sull'accesso AWS, vedi [Come accedere al tuo AWS account nella Guida per l'utente di AWS accesso](#).

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sulla firma delle richieste, consultare [Firma delle richieste AWS](#) nella Guida per l'utente IAM.

Indipendentemente dal metodo di autenticazione utilizzato, potrebbe esserti richiesto di fornire ulteriori informazioni di sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo 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 \(MFA\) AWS nella Guida per l'utente IAM](#).

AWS utente root dell'account

Quando si crea un AWS account, si inizia con un'identità di accesso che ha accesso completo a tutti i AWS servizi e le risorse dell'account. Questa identità è denominata utente root dell' AWS account ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Non usate mai l'utente root per le vostre attività quotidiane e prendete provvedimenti per salvaguardare le credenziali dell'utente root. Usali solo per eseguire attività che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente IAM.

Identità federata

È consigliabile richiedere agli utenti umani, compresi quelli che necessitano dell'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere ai AWS servizi utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, un provider di identità Web, il AWS Directory Service, la directory Identity Center o qualsiasi utente che accede AWS ai servizi utilizzando le credenziali fornite tramite un'origine di identità. Quando le identità federate accedono agli AWS account, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, ti consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutti i tuoi AWS account e applicazioni. Per 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 un'identità all'interno del tuo AWS account che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di fare affidamento su credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come password e chiavi di accesso. Se hai un caso d'uso specifico che richiede credenziali a lungo termine con utenti IAM, ti consigliamo 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 IAM.

Un [gruppo IAM](#) è un'identità che specifica una raccolta 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 di set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel 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 IAM.

Ruoli IAM

Un [ruolo IAM](#) è un'identità all'interno del tuo AWS account che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM nella console di AWS gestione [cambiando ruolo](#). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta [Utilizzo di ruoli IAM](#) nella Guida per l'utente 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 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, con alcuni AWS servizi, puoi allegare 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 [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente di IAM.
- **Accesso tra servizi**: alcuni AWS servizi utilizzano le funzionalità di altri AWS servizi. Ad esempio, quando si effettua 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.
 - **Ruolo di servizio** - Un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio da IAM. Per ulteriori informazioni, consultare [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'operazione per tuo conto. I

ruoli collegati al servizio vengono visualizzati nell' AWS account e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che effettuano richieste CLI o API AWS . AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile alle relative applicazioni, crei un profilo di 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 IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta [Quando creare un ruolo IAM \(invece di un utente\)](#) nella Guida per l'utente IAM.

Come AWS Security Incident Response funziona con IAM

AWS Identity and Access Management (IAM) è un AWS servizio che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS Security Incident Response IAM è un AWS servizio che puoi utilizzare senza costi aggiuntivi.

Funzionalità IAM che puoi utilizzare con AWS Security Incident Response	
<u>Funzionalità IAM</u>	<u>Allineamento dei servizi</u>
Policy basate sull'identità	Sì
Policy basate sulle risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi relative alle condizioni della politica	Sì (globale)
ACLs	No

Funzionalità IAM che puoi utilizzare con AWS Security Incident Response	
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	No
Ruoli collegati ai servizi	Sì

Indice

- [Politiche basate sull'identità per AWS Security Incident Response](#)
- [Chiavi relative alle condizioni politiche per AWS Security Incident Response](#)
- [Accedi agli elenchi di controllo \(ACLs\) in AWS Security Incident Response](#)

Politiche basate sull'identità per AWS Security Incident Response

Le policy basate sull'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 azioni 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 IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. 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.

Indice

- [Esempi di policy basate su identità](#)
- [Best practice per le policy](#)
- [Utilizzo della AWS Security Incident Response console](#)
- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)

- [Policy basate su risorse](#)
- [Operazioni di policy](#)

Esempi di policy basate su identità

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse. AWS Security Incident Response Inoltre, non possono eseguire attività utilizzando la console di AWS gestione, l'interfaccia a riga di AWS comando (AWS CLI) o AWS l'API. Un amministratore IAM può creare policy IAM per concedere agli utenti il permesso di eseguire azioni sulle risorse di cui hanno bisogno. 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 i dettagli sulle azioni e sui tipi di risorse definiti da AWS Security Incident Response, incluso il formato di ARNs per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione AWS Security Incident Response nel Service Authorization Reference.

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare AWS Security Incident Response risorse nel tuo account. Queste azioni possono comportare costi per il tuo account. AWS Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo account AWS . Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo policy gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente di IAM.

Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente di IAM.

Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite un AWS servizio specifico, ad esempio AWS CloudFormation. Per maggiori informazioni, consultare la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente di IAM.

Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. 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 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 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 AWS Security Incident Response console

Per accedere <https://console.aws.amazon.com/security-ir/>, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle AWS Security Incident Response risorse del tuo AWS account. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire le autorizzazioni minime della console per gli utenti che effettuano chiamate solo alla AWS CLI o AWS all'API. Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Allega la policy di AWS Security Incident Response accesso o ReadOnly AWS gestita per garantire che utenti e ruoli possano utilizzare la console di servizio. Per maggiori informazioni, consulta [Aggiunta di autorizzazioni a un utente](#) nella Guida per l'utente di IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o a livello di codice utilizzando la CLI o l'API AWS . AWS

Policy basate su risorse

Politiche basate sulle risorse nell'ambito di Security Incident Response AWS

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o servizi AWS .

Per ulteriori informazioni, consulta [Cross Account Resource Access in IAM nella IAM](#) User Guide.

Operazioni di policy

Azioni politiche per AWS Security Incident Response

Azioni politiche di supporto: Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento Azione di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le operazioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di AWS Security Incident Response azioni, vedere Azioni definite da AWS Security Incident Response nel Service Authorization Reference.

Le azioni politiche in AWS Security Incident Response uso utilizzano il seguente prefisso prima dell'azione:

AWS Security Incident Response -identità

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

«Azione»: ["AWS Security Incident Response -identity:action1"," -identity:action2"]AWS Security Incident Response

Risorse relative alle policy per Amazon AWS Security Incident Response

Supporta le risorse relative alle policy: Sì, gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento della policy Resource JSON specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere una risorsa o un NotResource elemento. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). È possibile eseguire questa operazione per operazioni 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": "*"

Chiavi relative alle condizioni politiche per AWS Security Incident Response

Supporta le chiavi di condizione delle policy specifiche del servizio: No

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento Condition (o blocco Condition) consente di specificare le condizioni in cui un'istruzione è valida. L'elemento condizione è facoltativo. È possibile compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specificate più elementi Condition in un'istruzione o più chiavi in un singolo elemento Condition, li AWS valuta utilizzando un'operazione AND logica. Se specificate 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.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile 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 IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'utente IAM.

Accedi agli elenchi di controllo (ACLs) in AWS Security Incident Response

Supporti ACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Controllo degli accessi basato sugli attributi (ABAC) con Security Incident Response AWS

Supporta ABAC (tag nelle policy): sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati 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 in base ai tag, fornisci le informazioni sui tag nell'[elemento condition](#) di una policy utilizzando le chiavi AWS: ResourceTag /key-name,: /key-name o AWS: RequestTag condition. AWS TagKeys Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale. Per ulteriori informazioni su ABAC, consulta [Che cos'è ABAC?](#) nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta [Utilizzo del controllo degli accessi basato su attributi \(ABAC\)](#) nella Guida per l'utente di IAM.

Credenziali temporanee con AWS Security Incident Response

Supporta le credenziali temporanee: sì

AWS i servizi non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi AWS i servizi che funzionano con credenziali temporanee, consulta [AWS i servizi che funzionano con IAM nella IAM User Guide](#). Stai utilizzando credenziali temporanee se accedi alla Console di AWS gestione utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente 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 IAM.

È possibile creare manualmente credenziali temporanee utilizzando la AWS CLI o l'API AWS . È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per maggiori informazioni, consulta [Credenziali di sicurezza provvisorie in IAM](#).

Sessioni di accesso diretto per AWS Security Incident Response

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un AWS servizio, in combinazione con il servizio richiedente per effettuare richieste ai AWS servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta [Forward access sessions](#).

Risoluzione dei problemi di AWS Security Incident Response identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con AWS Security Incident Response e IAM.

Argomenti

- Non sono autorizzato a eseguire un'operazione

- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne al mio AWS account di accedere alle mie AWS Security Incident Response risorse

Non sono autorizzato a eseguire alcuna azione

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.

Il seguente errore di esempio si verifica quando l'utente IAM mateojackson tenta di utilizzare la console per visualizzare i dettagli su una my-example-widget risorsa fittizia ma non dispone delle autorizzazioni AWS fittizie Security Incident Response:. GetWidget

Utente: arn ::iam: :123456789012:user/mateojackson non è autorizzato a eseguire:: on AWS resource: my -example-widget AWS Security Incident Response GetWidget

In questo caso, la politica per l'utente mateojackson deve essere aggiornata per consentire l'accesso alla risorsa utilizzando l'azione:. my-example-widget AWS Security Incident Response GetWidget

Se hai bisogno di aiuto, contatta il tuo 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 messaggio di errore indicante che non sei autorizzato a eseguire l'iam: PassRole azione iam:, le tue policy devono essere aggiornate per consentirti di assegnare un ruolo a AWS Security Incident Response .

Alcuni AWS servizi consentono di trasferire un ruolo esistente a quel servizio anziché 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 di nome marymajor tenta di utilizzare la console per eseguire un'azione in AWS Security Incident Response. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

User: arn ::iam: :123456789012:user/marymajor non è autorizzato a eseguire AWS: iam: PassRole

In questo caso, le politiche di Mary devono essere aggiornate per consentirle di eseguire l'azione iam:. PassRole Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne al mio AWS account di accedere alle mie AWS Security Incident Response 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 maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon AWS Security Incident Response supporta queste funzionalità, consulta [Come funziona AWS Security Incident Response con IAM](#).
- Per scoprire come fornire l'accesso alle tue risorse su tutti AWS gli account di tua proprietà, consulta [Fornire l'accesso a un utente IAM in un altro AWS account di tua proprietà](#) nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse ad AWS account di terze parti, consulta [Fornire l'accesso agli AWS account di proprietà di terze parti](#) nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(federazione delle identità\)](#) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente di IAM.

Utilizzo dei ruoli di servizio

Supporta i ruoli di servizio: no

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 [Creare un ruolo per delegare le autorizzazioni a un AWS servizio](#) nella Guida per l'utente IAM.

Uso di ruoli collegati ai servizi

Ruoli collegati ai servizi per AWS Security Incident Response

Indice

- [AWS SLR: AWSService RoleForSecurityIncidentResponse](#)
- [AWS SLR: AWSServiceRoleForSecurityIncidentResponse_Triage](#)
- [Regioni supportate per i ruoli collegati ai servizi AWS Security Incident Response](#)

Supporta i ruoli collegati ai servizi: Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un servizio. AWS Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account AWS e sono di proprietà del servizio. Un AWS Identity and Access Management amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

Un ruolo collegato al servizio semplifica la configurazione AWS Security Incident Response perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS Security Incident Response definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. AWS Security Incident Response Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni. Una policy delle autorizzazioni specifica non può essere collegata a un'altra entità IAM.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta i [AWS servizi che funzionano con IAM](#) e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

AWS SLR: AWSService RoleForSecurityIncidentResponse

AWS Security Incident Response utilizza la AWS Security Incident Response politica denominata AWSService RoleForSecurityIncidentResponse service-linked role (SLR) per identificare gli account sottoscritti, creare casi e etichettare le risorse correlate.

Permissions

Il ruolo AWSService RoleForSecurityIncidentResponse collegato al servizio si affida al seguente servizio per l'assunzione del ruolo:

- `triage.security-ir.amazonaws.com`

A questo ruolo è associata la politica AWS gestita denominata.

[AWSSecurityIncidentResponseServiceRolePolicy](#) Il servizio utilizza il ruolo per eseguire azioni sulle seguenti risorse:

- **AWS Organizations:** consente al servizio di cercare account di iscrizione da utilizzare con il servizio.
- **CreateCase:** consente al servizio di creare casi di servizio per conto degli account di iscrizione.
- **ListCases:** consente all'agente AI del servizio di visualizzare i casi ai fini delle indagini di sicurezza.

- **UpdateCase**: consente all'agente AI del servizio di aggiornare i metadati dei casi.
- **CreateCaseComment**: consente all'agente AI del servizio di pubblicare i risultati come commento al caso.
- **ListComments**: consente all'agente AI del servizio di visualizzare i commenti sui casi necessari per eseguire indagini automatizzate.
- **TagResource**: consente le risorse dei tag di servizio configurate come parte del servizio.

Gestione del ruolo

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando effettui l'onboarding per accedere AWS Security Incident Response a Console di gestione AWS AWS CLI, the o all' AWS API, il servizio crea automaticamente il ruolo collegato al servizio.

Note

Se hai creato un'iscrizione utilizzando un account amministratore delegato, i ruoli collegati al servizio devono essere creati manualmente negli account di gestione. AWS Organizations

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando ti iscrivi al servizio, il ruolo collegato al servizio viene nuovamente creato per te.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio è necessario configurare le relative autorizzazioni. Per ulteriori informazioni, consulta le [autorizzazioni dei ruoli collegati al servizio](#) nella Guida per l'utente IAM.

AWS SLR: AWSServiceRoleForSecurityIncidentResponse_Triage

AWS Security Incident Response utilizza la AWS Security Incident Response politica denominata AWSServiceRoleForSecurityIncidentResponse_Triage service-linked role (SLR) per monitorare continuamente l'ambiente alla ricerca di minacce alla sicurezza, ottimizzare i servizi di sicurezza per ridurre il rumore degli avvisi e raccogliere informazioni per indagare su potenziali incidenti.

Permissions

Il ruolo AWSServiceRoleForSecurityIncidentResponse_Triage collegato al servizio prevede che il ruolo venga svolto dal seguente servizio:

- `triage.security-ir.amazonaws.com`

A questo ruolo è associata la politica gestita AWS .

[AWSSecurityIncidentResponseTriageServiceRolePolicy](#) Il servizio utilizza il ruolo per eseguire azioni sulle seguenti risorse:

- **Eventi:** consente al servizio di creare una regola Amazon EventBridge gestita. Questa regola è l'infrastruttura richiesta nel tuo AWS account per inviare eventi dal tuo account al servizio. Questa azione viene eseguita su qualsiasi AWS risorsa gestita da `triage.security-ir.amazonaws.com`.
- **Amazon GuardDuty:** consente al servizio di ottimizzare i servizi di sicurezza per ridurre il rumore degli avvisi, raccogliere informazioni per indagare su potenziali incidenti e avviare scansioni di GuardDuty malware.
- **AWS Security Hub CSPM:** consente al servizio di elencare gli standard abilitati e le integrazioni di prodotti, elencare i membri dell'organizzazione e gli account degli amministratori e ottimizzare i servizi di sicurezza per ridurre il rumore degli avvisi e raccogliere informazioni per indagare su potenziali incidenti.
- **AWS Identity and Access Management:** consente al servizio di recuperare le informazioni sul ruolo `AWSServiceRoleForAmazonGuardDutyMalwareProtection` collegato al servizio per verificare se è configurato. `GuardDuty MalwareProtection`
- **AWS Security Incident Response:** Consente al servizio di creare e aggiornare casi e risorse di tag, limitatamente alle risorse contrassegnate con `SecurityIncidentResponseManaged=true`. Consente al servizio di leggere le informazioni sull'iscrizione (`GetMembership`, `ListMemberships`).

Gestire il ruolo

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando effettui l'onboarding per accedere AWS Security Incident Response a Console di gestione AWS AWS CLI, the o all' AWS API, il servizio crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando ti iscrivi al servizio, il ruolo collegato al servizio viene nuovamente creato per te.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio è necessario configurare le relative autorizzazioni. Per ulteriori informazioni, consulta le [autorizzazioni dei ruoli collegati al servizio](#) nella Guida per l'utente IAM.

Regioni supportate per i ruoli collegati ai servizi AWS Security Incident Response

AWS Security Incident Response supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile.

- Stati Uniti orientali (Ohio)
- Stati Uniti occidentali (Oregon)
- Stati Uniti orientali (Virginia)
- Europa (Francoforte)
- Europa (Irlanda)
- Europa (Londra)
- Europa (Milano)
- Europa (Parigi)
- Europa (Spagna)
- Europa (Stoccolma)
- Europa (Zurigo)
- Asia Pacifico (Hong Kong)
- Asia Pacifico (Hyderabad)
- Asia Pacifico (Giacarta)
- Asia Pacifico (Melbourne)
- Asia Pacifico (Mumbai)
- Asia Pacifico (Seoul)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Tokyo)
- Canada (Centrale)
- Medio Oriente (Bahrein)
- Medio Oriente (Emirati Arabi Uniti)
- Sud America (San Paolo)
- Africa (Città del Capo)

AWS Policy gestite

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le policy AWS gestite che scriverle da soli. La [creazione di policy gestite dai clienti IAM](#) che forniscono al team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste politiche coprono casi d'uso comuni e sono disponibili nel tuo AWS account. 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 associate. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS 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 policy gestita da AWS quando viene avviata 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, consultare la sezione [Policy gestite da AWS per funzioni di processi](#) nella Guida per l'utente di IAM.

Indice

- [AWS politica gestita: AWSSecurity IncidentResponseServiceRolePolicy](#)
- [AWS politica gestita: AWSSecurity IncidentResponseFullAccess](#)
- [AWS politica gestita: AWSSecurity IncidentResponseReadOnlyAccess](#)
- [AWS politica gestita: AWSSecurity IncidentResponseCaseFullAccess](#)
- [AWS politica gestita: AWSSecurity IncidentResponseTriageServiceRolePolicy](#)
- [AWS Security Incident Response aggiornamenti SLRs e politiche gestite](#)

AWS politica gestita: AWSSecurity IncidentResponseServiceRolePolicy

AWS Security Incident Response utilizza la politica AWSSecurity IncidentResponseServiceRolePolicy AWS gestita. Questa policy AWS gestita è associata al ruolo [AWSServiceRoleForSecurityIncidentResponse](#) collegato al servizio. La policy fornisce l'accesso AWS Security Incident Response per identificare gli account sottoscritti, creare casi, aggiornare casi, creare commenti sui casi, elencare casi, elencare i commenti sui casi e inserire le risorse relative ai tag.

Important

Non archiviate informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. AWS Security Incident Response utilizza i tag per fornirti servizi di amministrazione. I tag non sono pensati per essere utilizzati per dati privati o sensibili

Dettagli delle autorizzazioni

Il servizio utilizza questa politica per eseguire azioni sulle seguenti risorse:

- **AWS Organizations:** consente al servizio di cercare account di iscrizione da utilizzare con il servizio.
- **CreateCase:** consente al servizio di creare casi di servizio per conto degli account di iscrizione.
- **ListCases:** consente all'agente AI del servizio di visualizzare i casi ai fini delle indagini di sicurezza.
- **UpdateCase:** consente all'agente AI del servizio di aggiornare i metadati dei casi.
- **CreateCaseComment:** consente all'agente AI del servizio di pubblicare i risultati come commento al caso.
- **ListComments:** consente all'agente AI del servizio di visualizzare i commenti sui casi necessari per eseguire indagini automatizzate.
- **TagResource:** consente le risorse dei tag di servizio configurate come parte del servizio.

È possibile visualizzare le autorizzazioni associate a questa politica nelle politiche AWS gestite per [AWSSecurityIncidentResponseServiceRolePolicy](#).

AWS politica gestita: AWSSecurity IncidentResponseFullAccess

AWS Security Incident Response utilizza la politica AWSSecurity IncidentResponseAdmin AWS gestita. Questa politica garantisce l'accesso completo alle risorse del servizio e l'accesso alle risorse correlate Servizi AWS. Puoi utilizzare questa policy con i tuoi responsabili IAM per aggiungere rapidamente le autorizzazioni per. AWS Security Incident Response

Important

Non archiviate informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. AWS Security Incident Response utilizza i tag per fornirti servizi di amministrazione. I tag non sono pensati per essere utilizzati per dati privati o sensibili

Dettagli delle autorizzazioni

Il servizio utilizza questa politica per eseguire azioni sulle seguenti risorse:

- Accesso in sola lettura principale IAM: concede a un utente del servizio la possibilità di eseguire azioni di sola lettura sulle risorse esistenti. AWS Security Incident Response
- Accesso di scrittura principale IAM: concede a un utente del servizio la possibilità di aggiornare, modificare, eliminare e creare risorse. AWS Security Incident Response

È possibile visualizzare le autorizzazioni associate a questa politica nelle politiche AWS gestite per. [AWSSecurityIncidentResponseFullAccess](#)

AWS politica gestita: AWSSecurity IncidentResponseReadOnlyAccess

AWS Security Incident Response utilizza la politica AWSSecurity IncidentResponseReadOnlyAccess AWS gestita. La policy concede l'accesso in sola lettura alle risorse dei service case. Puoi utilizzare questa policy con i tuoi presidi IAM per aggiungere rapidamente le autorizzazioni per. AWS Security Incident Response

Important

Non archiviate informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. AWS Security Incident Response utilizza i tag per fornirti servizi di amministrazione. I tag non sono pensati per essere utilizzati per dati privati o sensibili

Dettagli delle autorizzazioni

Il servizio utilizza questa politica per eseguire azioni sulle seguenti risorse:

- Accesso in sola lettura principale IAM: concede a un utente del servizio la possibilità di eseguire azioni di sola lettura sulle risorse esistenti. AWS Security Incident Response

È possibile visualizzare le autorizzazioni associate a questa policy nelle policy gestite per. [AWS Security Incident Response Read Only Access](#)

AWS politica gestita: AWS Security Incident Response Case Full Access

AWS Security Incident Response utilizza la politica AWS Security Incident Response Case Full Access AWS gestita. La policy garantisce l'accesso completo alle risorse dei service case. Puoi utilizzare questa policy con i tuoi presidi IAM per aggiungere rapidamente le autorizzazioni per. AWS Security Incident Response

Important

Non archiviate informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. AWS Security Incident Response utilizza i tag per fornirti servizi di amministrazione. I tag non sono pensati per essere utilizzati per dati privati o sensibili

Dettagli delle autorizzazioni

Il servizio utilizza questa politica per eseguire azioni sulle seguenti risorse:

- Accesso in sola lettura ai casi principali IAM: concede a un utente del servizio la possibilità di eseguire azioni di sola lettura su casi esistenti. AWS Security Incident Response
- Accesso alla scrittura sui casi principali IAM: concede a un utente del servizio la possibilità di aggiornare, modificare, eliminare e creare casi. AWS Security Incident Response

È possibile visualizzare le autorizzazioni associate a questa policy nelle politiche AWS gestite per. [AWS Security Incident Response Case Full Access](#)

AWS politica gestita: AWSSecurity IncidentResponseTriageServiceRolePolicy

AWS Security Incident Response utilizza la politica AWSSecurity IncidentResponseTriageServiceRolePolicy AWS gestita. Questa policy AWS gestita è associata al ruolo [AWSServiceRoleForSecurityIncidentResponse_Triage](#) collegato al servizio.

La policy consente di monitorare continuamente l'ambiente per rilevare eventuali minacce AWS Security Incident Response alla sicurezza, ottimizzare i servizi di sicurezza per ridurre il rumore generato dagli allarmi e raccogliere informazioni per indagare su potenziali incidenti. Non è possibile attribuire questa policy alle entità IAM.

Important

Non archiviate informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. AWS Security Incident Response utilizza i tag per fornirti servizi di amministrazione. I tag non sono pensati per essere utilizzati per dati privati o sensibili

Dettagli delle autorizzazioni

Il servizio utilizza questa politica per eseguire azioni sulle seguenti risorse:

- **Eventi:** consente al servizio di creare una regola EventBridge gestita da Amazon. Questa regola è l'infrastruttura richiesta nel tuo AWS account per inviare eventi dal tuo account al servizio. Questa azione viene eseguita su qualsiasi AWS risorsa gestita da `trriage.security-ir.amazonaws.com`.
- **Amazon GuardDuty:** consente al servizio di ottimizzare i servizi di sicurezza per ridurre il rumore degli avvisi, raccogliere informazioni per indagare su potenziali incidenti e avviare scansioni di GuardDuty malware.
- **AWS Security Hub CSPM:** consente al servizio di elencare gli standard abilitati e le integrazioni di prodotti, elencare i membri dell'organizzazione e gli account degli amministratori e ottimizzare i servizi di sicurezza per ridurre il rumore degli avvisi e raccogliere informazioni per indagare su potenziali incidenti.
- **AWS Identity and Access Management:** consente al servizio di recuperare le informazioni sul ruolo `AWSServiceRoleForAmazonGuardDutyMalwareProtection` collegato al servizio per verificare se è configurato. GuardDuty MalwareProtection

- **AWS Security Incident Response:** Consente al servizio di creare e aggiornare casi e risorse di tag, limitatamente alle risorse contrassegnate con `SecurityIncidentResponseManaged=true`. Consente al servizio di leggere le informazioni sull'iscrizione (`GetMembership`, `ListMemberships`).

È possibile visualizzare le autorizzazioni associate a questa politica nelle politiche AWS gestite per [AWSSecurityIncidentResponseTriageServiceRolePolicy](#).

AWS Security Incident Response aggiornamenti SLRs e politiche gestite

Visualizza i dettagli sugli aggiornamenti AWS Security Incident Response SLRs e sui ruoli delle politiche gestite da quando questo servizio ha iniziato a tenere traccia di queste modifiche.

Modifica	Descrizione	Data
Aggiornato: AWSSecurityIncidentResponseTriageServiceRolePolicy	La policy ora consente al servizio di modificare GuardDuty i filtri contrassegnati con <code>SecurityIncidentResponseManaged=true</code> , di aggiornare le configurazioni dei rilevatori e di avviare GuardDuty scansioni antimalware. Consente al servizio di creare e gestire regole che agiscono automaticamente sui risultati del Security Hub CSPM e di comprendere la struttura organizzativa.	27 marzo 2026
Aggiornato — AWSSecurityIncidentResponseServiceRolePolicy	La politica ora esegue azioni sulle seguenti risorse: ListCases: consente all'agente AI del servizio di visualizzare i casi ai fini delle indagini di sicurezza UpdateCase: consente all'agente AI del servizio di aggiornare i metadati dei casi. CreateCaseComment: consente all'agente AI del servizio di pubblicare i risultati come commento al caso ListComments: consente all'agente AI del servizio di visualizzare i commenti sui casi necessari per eseguire indagini automatizzate	Novembre 2025

Modifica	Descrizione	Data
<p>Aggiornato: AWS Security Incident Response Service Role Policy</p>	<p>La politica ora include due nuove azioni "organizations:DescribeAccount" "organizations:ListDelegatedAdministrators" e una nuova condizione:</p> <pre data-bbox="402 422 1219 821"> "Condition": { "StringEquals": { "aws:ResourceAccount": "\${aws:PrincipalAccount}" } }</pre>	<p>Novembre 2025</p>
<p>Aggiornamenti a SLR che aggiungono autorizzazioni ai diritti del servizio di supporto.</p>	<p>AWS Security Incident Response Triage Service Role Policy è stato aggiornato per aggiungere security-ir:GetMemberships, security-ir:, security-ir:, guardduty:, guardduty: ListMemberships, guardduty: e guardduty: UpdateCase e guardduty: permissions. guardduty: ListFilters è stato aggiunto per facilitare la gestione UpdateFilter dei filtri di archiviazione automatica negli account DeleteFilter delegati. GetAdministratorAccount GetAdministratorAccount GuardDuty</p>	<p>02 giugno 2025</p>

Modifica	Descrizione	Data
<p>Nuova reflex — AWSServiceRoleForSecurityIncidentResponse</p> <p>Nuova politica gestita: AWSSecurityIncidentResponseServiceRolePolicy.</p>	<p>Nuovo ruolo collegato al servizio e policy allegata che consentono l'accesso del servizio AWS Organizations agli account per identificare l'appartenenza.</p>	<p>1 dicembre 2024</p>
<p>Nuova reflex — AWSServiceRoleForSecurityIncidentResponse_Triage</p> <p>Nuova politica gestita — AWSSecurityIncidentResponseTriageServiceRolePolicy</p>	<p>Nuovo ruolo collegato al servizio e policy allegata che consentono l'accesso del servizio AWS Organizations agli account per eseguire la valutazione degli eventi di sicurezza.</p>	<p>1 dicembre 2024</p>
<p>Nuova politica gestita: AWSSecurityIncidentResponseFullAccess</p>	<p>AWS Security Incident Response aggiungi una nuova reflex da collegare ai principali IAM per le azioni di lettura e scrittura del servizio.</p>	<p>1 dicembre 2024</p>

Modifica	Descrizione	Data
Nuovo ruolo di policy gestita: AWSSecurityIncidentResponseReadOnlyAccess	AWS Security Incident Response aggiungi una nuova reflex da collegare ai principi IAM per le azioni di lettura	1 dicembre 2024
Nuovo ruolo di policy gestita: AWSSecurityIncidentResponseCaseFullAccess	AWS Security Incident Response aggiungi una nuova reflex da collegare ai principi IAM per le azioni di lettura e scrittura per i service case.	1 dicembre 2024
Ha iniziato a tenere traccia delle modifiche.	Ha iniziato a tenere traccia delle modifiche AWS Security Incident Response SLRs e a gestire le politiche	1 dicembre 2024

Risposta agli incidenti

La sicurezza e la conformità sono una responsabilità condivisa tra AWS e il cliente. Questo modello condiviso può contribuire ad alleggerire l'onere operativo del cliente in quanto AWS opera, gestisce e controlla i componenti, dal sistema operativo host e dal livello di virtualizzazione fino alla sicurezza fisica delle strutture in cui opera il servizio. Il cliente si assume la responsabilità e la gestione del sistema operativo guest (inclusi gli aggiornamenti e le patch di sicurezza), degli altri software applicativi associati e della configurazione del firewall del gruppo di sicurezza AWS fornito. Per ulteriori informazioni, fare riferimento al modello di [responsabilitàAWS condivisa](#).

Stabilendo una linea di base di sicurezza che soddisfi gli obiettivi delle applicazioni eseguite nel cloud, l'utente è in grado di rilevare deviazioni a cui è possibile rispondere. Poiché la risposta agli incidenti di sicurezza può essere un argomento complesso, ti invitiamo a consultare le seguenti risorse in modo da comprendere meglio l'impatto che la risposta agli incidenti e le tue scelte hanno sugli obiettivi aziendali: white paper sulle [migliori pratiche di AWS sicurezza](#) e white paper sulla [prospettiva della sicurezza del AWS cloud Adoption Framework \(CAF\)](#).

Convalida della conformità

I revisori di terze parti valutano la sicurezza e la conformità dei AWS servizi nell'ambito di più programmi di conformità. AWS Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per un elenco dei AWS servizi che rientrano nell'ambito di specifici programmi di conformità, consulta la sezione [AWS Servizi rientranti nell'ambito del programma di conformità](#). Per informazioni generali, consulta i programmi di AWS conformità.

Puoi scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Scaricamento dei report in AWS Artifact](#).

La responsabilità dell'utente in materia di conformità nell'utilizzo dei AWS servizi è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- [Guide introduttive su sicurezza e conformità](#): queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla sicurezza e la conformità. AWS
- [Whitepaper sull'architettura per la sicurezza e la conformità HIPAA: questo white paper](#) descrive in che modo le aziende possono utilizzare per creare applicazioni conformi allo standard HIPAA. AWS
- [AWS risorse per la conformità](#): una raccolta di cartelle di lavoro e guide applicabili in base all'area geografica del settore. and/or
- [Valutazione delle risorse con AWS Config Rules nella AWS Config Developer Guide](#) — AWS Config; valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- [AWS Security Hub](#): questo AWS servizio offre una visione completa dello stato di sicurezza interno AWS. Security Hub utilizza i controlli di sicurezza per valutare le AWS risorse e verificare la conformità rispetto 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](#).
- [Amazon GuardDuty](#): questo AWS servizio rileva potenziali minacce ai tuoi AWS account, carichi di lavoro, contenitori e dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.

- [AWS Audit Manager](#): questo AWS servizio consente di verificare continuamente AWS l'utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Registrazione e monitoraggio in AWS Security Incident Response

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle AWS Security Incident Response altre AWS soluzioni esistenti. AWS Security Incident Response attualmente supporta i seguenti AWS servizi per monitorare l'organizzazione e l'attività che si svolge al suo interno.

AWS CloudTrail — Con CloudTrail è possibile acquisire chiamate API dalla console AWS Security Incident Response. Ad esempio, quando un utente si autentica, CloudTrail può registrare dettagli come l'indirizzo IP nella richiesta, chi ha effettuato la richiesta e quando è stata effettuata.

Amazon CloudWatch Metrics: con le CloudWatch metriche puoi monitorare, segnalare e intraprendere azioni automatiche in caso di evento quasi in tempo reale. Ad esempio, puoi creare CloudWatch dashboard sulle metriche fornite per monitorare l' AWS Security Incident Response utilizzo oppure creare CloudWatch allarmi in base ai parametri forniti per avvisarti in caso di violazione di una soglia prestabilita.

Lo spazio dei nomi per il servizio è `/Usage/`. AWS ServiceName I nomi delle metriche disponibili sono `e.ActiveManagedCases` `SelfManagedCases`

In conformità con i [Termini di AWS servizio](#), il team AWS Security Incident Response di risposta avrà accesso alla cronologia dei dati di registro VPC CloudTrail, DNS e S3. Questi dati possono essere utilizzati durante incidenti di sicurezza attivi quando un caso è aperto nel portale del servizio Security Incident Response. AWS

Resilienza

L'infrastruttura AWS globale è costruita attorno a AWS regioni 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 tradizionali.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta [infrastruttura AWS globale](#).

Sicurezza dell'infrastruttura

AWS Security Incident Response è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta [AWS Cloud Security](#). Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere AWS Security Incident Response attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di 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. Oppure puoi utilizzare il [AWS Security Token Service](#) (AWS STS) per generare credenziali di sicurezza temporanee per firmare le richieste.

Analisi della configurazione e delle vulnerabilità

Sei responsabile della gestione dei ruoli di contenimento del servizio e dei set di CloudFormation stack associati.

AWS gestisce le attività di sicurezza di base, come l'applicazione di patch al sistema operativo (OS) guest e al database, la configurazione del firewall e il disaster recovery. Queste procedure sono state riviste e certificate dalle terze parti appropriate. Per ulteriori dettagli, consulta le seguenti risorse AWS :

- [Modello di responsabilità condivisa](#)
- [Best practice per sicurezza, identità e conformità.](#)

Prevenzione del problema "confused deputy" tra servizi

Il problema confused deputy è un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire un'azione può costringere un'entità maggiormente privilegiata a eseguire l'azione. Nel frattempo AWS, l'impersonificazione tra servizi può portare al confuso

problema del vicesceriffo. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare che ciò accada, AWS mette a disposizione strumenti che consentono di proteggere i dati relativi a tutti i servizi con responsabili del servizio a cui è stato concesso l'accesso alle risorse del vostro account.

Ti consigliamo di utilizzare le chiavi di contesto [AWSAWS: SourceArn and: SourceAccount](#) global condition nelle politiche delle risorse per limitare le autorizzazioni che Amazon Connect concede a un altro servizio alla risorsa. Se utilizzi entrambe le chiavi di contesto della condizione globale, il SourceAccount valore AWS: e l'account nel SourceArn valore AWS: devono utilizzare lo stesso ID account quando vengono utilizzati nella stessa dichiarazione politica.

Il modo più efficace per proteggersi dal problema "confused deputy" è utilizzare il nome della risorsa Amazon (ARN) esatto della risorsa che vuoi autorizzare. Se non conosci l'ARN completo della risorsa o se stai specificando più risorse, usa la chiave AWS: SourceArn global context condition con caratteri jolly (*) per le parti sconosciute dell'ARN. Ad esempio, arn ::servicename: :region-name: :your account ID AWS: *. AWS

[Per un esempio di politica di assunzione del ruolo che mostra come prevenire la confusione dei deputati, vedi Politica di prevenzione dei deputati confusi.](#)

Service Quotas

AWS Security Incident Response

La Guida di riferimento AWS generale include gli [AWS Security Incident Response endpoint e le quote](#) più recenti.

AWS Security Incident Response Guida tecnica

Indice

- [Sintesi](#)
- [Sei Well-Architected?](#)
- [Introduzione](#)
- [Preparazione](#)
- [Operazioni](#)
- [Attività post-incidente](#)
- [Conclusioni](#)
- [Collaboratori](#)
- [Appendice A: Definizioni delle funzionalità cloud](#)
- [Appendice B: AWS risorse per la risposta agli incidenti](#)
- [Note](#)

Sintesi

Questa guida presenta una panoramica dei fondamenti per rispondere agli incidenti di sicurezza all'interno dell'ambiente Amazon Web Services (AWS) Cloud di un cliente. Fornisce una panoramica dei concetti di sicurezza del cloud e di risposta agli incidenti e identifica le funzionalità, i servizi e i meccanismi cloud a disposizione dei clienti che devono rispondere a problemi di sicurezza.

Questa guida è destinata a chi ricopre ruoli tecnici e presuppone che l'utente conosca i principi generali della sicurezza delle informazioni, abbia una conoscenza di base della risposta agli incidenti di sicurezza negli attuali ambienti locali e abbia una certa familiarità con i servizi cloud.

Sei Well-Architected?

Il [AWS Well-Architected](#) Framework ti aiuta a comprendere i pro e i contro delle decisioni che prendi quando crei sistemi nel cloud. I sei pilastri del Framework consentono di apprendere le migliori pratiche architettoniche per progettare e gestire sistemi affidabili, sicuri, efficienti, convenienti e sostenibili. Utilizzando [AWS Well-Architected Tool](#), disponibile gratuitamente nella [AWS Well-](#)

[Architected Tool console](#), puoi esaminare i tuoi carichi di lavoro rispetto a queste best practice rispondendo a una serie di domande per ogni pilastro.

[Per ulteriori indicazioni e best practice da parte degli esperti per la tua architettura cloud \(implementazioni dell'architettura di riferimento, diagrammi e white paper\), consulta l'Architecture Center.AWS](#)

Introduzione

La sicurezza è la massima priorità in AWS. AWS i clienti traggono vantaggio dai data center e dall'architettura di rete progettati per supportare le esigenze delle organizzazioni più sensibili alla sicurezza. AWS ha un modello di responsabilità AWS condivisa: gestisce la sicurezza del cloud e i clienti sono responsabili della sicurezza nel cloud. Ciò significa che avete il pieno controllo dell'implementazione della sicurezza, incluso l'accesso a diversi strumenti e servizi per aiutarvi a raggiungere i vostri obiettivi di sicurezza. Queste funzionalità consentono di stabilire una base di sicurezza per le applicazioni in esecuzione in Cloud AWS

Quando si verifica una deviazione dalla linea di base, ad esempio a causa di una configurazione errata o della modifica di fattori esterni, è necessario reagire e indagare. Per farlo con successo, è necessario comprendere i concetti di base della risposta agli incidenti di sicurezza all'interno del proprio AWS ambiente e i requisiti per preparare, istruire e formare i team cloud prima che si verifichino problemi di sicurezza. È importante sapere quali controlli e funzionalità è possibile utilizzare, esaminare esempi di attualità per risolvere potenziali problemi e identificare i metodi di riparazione che utilizzano l'automazione per migliorare la velocità e la coerenza di risposta. Inoltre, è necessario comprendere i requisiti normativi e di conformità relativi alla creazione di un programma di risposta agli incidenti di sicurezza che soddisfi tali requisiti.

La risposta agli incidenti di sicurezza può essere complessa, quindi ti invitiamo a implementare un approccio iterativo: iniziare con i servizi di sicurezza di base, sviluppare funzionalità di rilevamento e risposta di base, quindi sviluppare dei playbook per creare una libreria iniziale di meccanismi di risposta agli incidenti su cui iterare e migliorare.

Prima di iniziare

Prima di iniziare a conoscere la risposta agli incidenti per gli eventi di sicurezza in AWS, acquisite familiarità con gli standard e i framework pertinenti per la sicurezza e la risposta agli incidenti. AWS Queste basi ti aiuteranno a comprendere i concetti e le migliori pratiche presentati in questa guida.

AWS standard e framework di sicurezza

Per iniziare, ti invitiamo a leggere il white paper [Best Practices for Security, Identity, and Compliance, Security Pillar - AWS Well-Architected Framework](#) e [Security Perspective of the Overview of AWS the Cloud Adoption Framework AWS \(CAF\)](#).

Il AWS CAF fornisce linee guida a supporto del coordinamento tra le diverse parti delle organizzazioni che passano al cloud. La guida AWS CAF è suddivisa in diverse aree di interesse, denominate prospettive, che sono rilevanti per la creazione di sistemi IT basati sul cloud. La prospettiva della sicurezza descrive come implementare un programma di sicurezza tra i flussi di lavoro, uno dei quali è la risposta agli incidenti. Questo documento è il prodotto delle nostre esperienze di collaborazione con i clienti per aiutarli a creare programmi e funzionalità di risposta agli incidenti di sicurezza efficaci ed efficienti.

Standard e framework di risposta agli incidenti di settore

Questo white paper segue gli standard di risposta agli incidenti e le migliori pratiche della [Computer Security Incident Handling Guide SP 800-61 r3](#), creata dal National Institute of Standards and Technology (NIST). Leggere e comprendere i concetti introdotti dal NIST è un utile prerequisito. I concetti e le migliori pratiche di questa guida del NIST verranno applicati alle AWS tecnologie in questo paper. Tuttavia, gli scenari di incidenti in sede non rientrano nell'ambito di questa guida.

AWS panoramica della risposta agli incidenti

Per iniziare, è importante capire in che modo le operazioni di sicurezza e la risposta agli incidenti sono diverse nel cloud. Per sviluppare funzionalità di risposta efficaci in AWS, è necessario comprendere le deviazioni dalla tradizionale risposta locale e il loro impatto sul programma di risposta agli incidenti. Ciascuna di queste differenze, nonché i principi fondamentali di progettazione della risposta agli AWS incidenti, sono descritti in dettaglio in questa sezione.

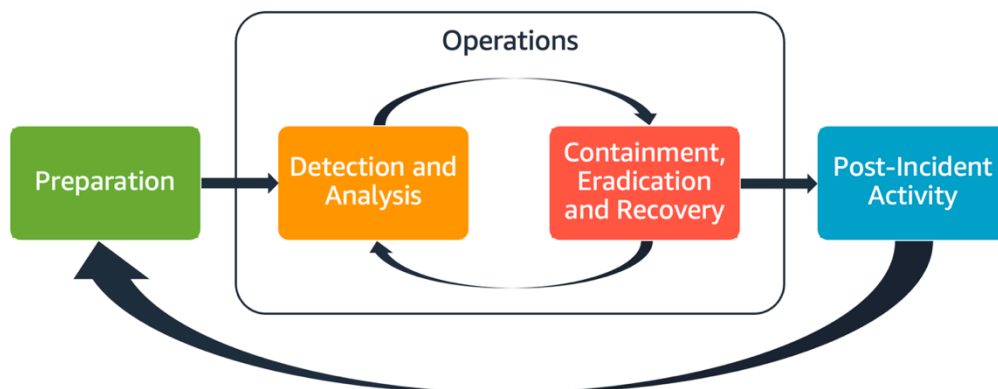
Aspetti della risposta AWS agli incidenti

Tutti AWS gli utenti di un'organizzazione devono avere una conoscenza di base dei processi di risposta agli incidenti di sicurezza e il personale addetto alla sicurezza deve capire come rispondere ai problemi di sicurezza. L'istruzione, la formazione e l'esperienza sono fondamentali per un programma di risposta agli incidenti nel cloud efficace e idealmente sono implementate con largo anticipo rispetto alla gestione di un possibile incidente di sicurezza. La base di un programma di risposta agli incidenti di successo nel cloud è la preparazione, le operazioni e l'attività post-incidente.

Per comprendere ciascuno di questi aspetti, considera le seguenti descrizioni:

- **Preparazione:** prepara il tuo team di risposta agli incidenti a rilevare e rispondere agli incidenti internamente AWS abilitando i controlli investigativi e verificando l'accesso appropriato agli strumenti e ai servizi cloud necessari. Inoltre, prepara i playbook necessari, sia manuali sia automatizzati, per verificare che le risposte siano affidabili e coerenti.
- **Operazioni:** gestisci gli eventi di sicurezza e i potenziali incidenti seguendo le fasi di risposta agli incidenti del NIST: rilevamento, analisi, contenimento, eliminazione e ripristino.
- **Attività post-incidente:** esegui iterazioni sull'esito degli eventi e delle simulazioni di sicurezza per migliorare l'efficacia della risposta, aumentare il valore derivante dalla risposta e dalle indagini e ridurre ulteriormente i rischi. Impara dagli incidenti e dimostra una forte responsabilità verso le attività di miglioramento.

Ciascuno di questi aspetti viene esplorato e dettagliato in questa guida. Il diagramma seguente mostra il flusso di questi aspetti, in linea con il ciclo di vita della risposta agli incidenti del NIST menzionato in precedenza, ma con operazioni che comprendono il rilevamento e l'analisi con il contenimento, l'eradicazione e il ripristino.



Aspetti della risposta AWS agli incidenti

AWS principi di risposta agli incidenti e obiettivi di progettazione

Sebbene i processi e i meccanismi generali di risposta agli incidenti definiti dalla [Guida alla gestione degli incidenti di sicurezza informatica NIST SP 800-61](#) siano validi, ti invitiamo a considerare anche questi obiettivi di progettazione specifici che sono rilevanti per rispondere agli incidenti di sicurezza in un ambiente cloud:

- **Stabilire gli obiettivi di risposta:** collaborare con le parti interessate, i consulenti legali e i dirigenti organizzativi per determinare l'obiettivo della risposta a un incidente. Alcuni obiettivi comuni includono il contenimento e la mitigazione del problema, il recupero delle risorse interessate, la

conservazione dei dati per le indagini forensi, il ripristino delle operazioni sicure note e, in ultima analisi, l'apprendimento dagli incidenti.

- Rispondi utilizzando il cloud: implementa modelli di risposta all'interno del cloud, dove si verificano l'evento e i dati.
- Scopri cosa hai e di cosa hai bisogno: conserva registri, risorse, istantanee e altre prove copiandoli e archiviandoli in un account cloud centralizzato dedicato alla risposta. Utilizza tag, metadati e meccanismi che applicano le policy di conservazione. Dovrai capire quali servizi utilizzi e quindi identificare i requisiti per esaminarli. Per aiutarvi a comprendere l'ambiente in uso, potete anche utilizzare i tag, come illustrato più avanti in questo documento nella [the section called “Sviluppa e implementa una strategia di assegnazione tag”](#) sezione.
- Utilizza meccanismi di redistribuzione: se un'anomalia di sicurezza può essere attribuita a una configurazione errata, la correzione potrebbe essere semplice: basta rimuovere la varianza redistribuendo le risorse con la configurazione corretta. Se viene identificato un possibile compromesso, verificate che la redistribuzione includa una mitigazione corretta e verificata delle cause principali.
- Automatizza laddove possibile: man mano che sorgono problemi o si ripetono gli incidenti, crea meccanismi per il triage programmatico e la risposta agli eventi comuni. Utilizza le risposte umane per incidenti unici, complessi o sensibili in cui le automazioni sono insufficienti.
- Scegliete soluzioni scalabili: cercate di eguagliare la scalabilità dell'approccio della vostra organizzazione al cloud computing. Implementa meccanismi di rilevamento e risposta scalabili tra i tuoi ambienti per ridurre efficacemente il tempo tra il rilevamento e la risposta.
- Impara e migliora il tuo processo: sii proattivo nell'identificare le lacune nei tuoi processi, strumenti o persone e implementa un piano per risolverle. Le simulazioni sono metodi sicuri per individuare lacune e migliorare i processi. Consultate la [the section called “Attività post-incidente”](#) sezione di questo documento per i dettagli su come iterare i processi.

Questi obiettivi di progettazione sono un promemoria per rivedere l'implementazione dell'architettura al fine di migliorare la capacità di condurre sia la risposta agli incidenti sia il rilevamento delle minacce. Mentre pianifichi le tue implementazioni cloud, pensa a rispondere a un incidente, idealmente con una metodologia di risposta valida dal punto di vista forense. In alcuni casi, ciò significa che potresti avere più organizzazioni, account e strumenti configurati specificamente per queste attività di risposta. Questi strumenti e funzioni devono essere messi a disposizione del team di risposta agli incidenti tramite una pipeline di implementazione. Non devono essere statici perché possono causare un rischio maggiore.

Domini relativi agli incidenti di sicurezza nel cloud

Per prepararsi e rispondere efficacemente agli eventi di sicurezza nel proprio AWS ambiente, è necessario comprendere i tipi più comuni di incidenti di sicurezza nel cloud. Esistono tre domini di responsabilità del cliente in cui potrebbero verificarsi incidenti di sicurezza: servizio, infrastruttura e applicazione. Domini diversi richiedono conoscenze, strumenti e processi di risposta diversi.

Considera questi domini:

- **Dominio di servizio:** gli incidenti nel dominio del servizio potrebbero influire sulle autorizzazioni [AWS Identity and Access Management \(IAM\)](#) Account AWS, sui metadati delle risorse, sulla fatturazione o su altre aree. Un evento del dominio di servizio è un evento a cui rispondi esclusivamente con meccanismi AWS API o in cui le cause principali sono associate alla configurazione o alle autorizzazioni delle risorse e potresti avere una registrazione correlata orientata ai servizi.
- **Dominio dell'infrastruttura:** gli incidenti nel dominio dell'infrastruttura includono dati o attività relative alla rete, come processi e dati sulle istanze [Amazon Elastic Compute Cloud \(Amazon EC2\)](#), traffico verso le istanze Amazon EC2 all'interno del cloud privato virtuale (VPC) e altre aree, come contenitori o altri servizi futuri. La tua risposta agli eventi del dominio dell'infrastruttura spesso implica l'acquisizione di dati relativi agli incidenti per l'analisi forense. Probabilmente include l'interazione con il sistema operativo di un'istanza e, in diversi casi, potrebbe anche coinvolgere meccanismi API. AWS Nel dominio dell'infrastruttura, puoi utilizzare una combinazione di AWS API e strumenti di forensics/incident risposta digitale (DFIR) all'interno di un sistema operativo guest, ad esempio un'istanza Amazon EC2 dedicata all'esecuzione di analisi e indagini forensi. Gli incidenti relativi al dominio dell'infrastruttura potrebbero comportare l'analisi dell'acquisizione di pacchetti di rete, dei blocchi di dischi su un volume [Amazon Elastic Block Store \(Amazon EBS\)](#) o della memoria volatile acquisita da un'istanza.
- **Dominio dell'applicazione:** gli incidenti nel dominio dell'applicazione si verificano nel codice dell'applicazione o nel software distribuito nei servizi o nell'infrastruttura. Questo dominio deve essere incluso nei playbook di rilevamento e risposta alle minacce nel cloud e potrebbe includere risposte simili a quelle del dominio dell'infrastruttura. Con un'architettura applicativa appropriata e ponderata, puoi gestire questo dominio con strumenti cloud utilizzando l'acquisizione, il ripristino e la distribuzione automatizzati.

In questi domini, considera gli attori che potrebbero agire contro AWS account, risorse o dati. Che sia interno o esterno, utilizza un framework di rischio per determinare i rischi specifici per l'organizzazione e prepararti di conseguenza. Inoltre, dovreste sviluppare modelli di minaccia che possano aiutarvi a pianificare la risposta agli incidenti e a costruire un'architettura ponderata.

Principali differenze nella risposta agli incidenti in AWS

La risposta agli incidenti è parte integrante di una strategia di sicurezza informatica locale o nel cloud. I principi di sicurezza come il privilegio minimo e la difesa approfondita mirano a proteggere la riservatezza, l'integrità e la disponibilità dei dati sia in locale che nel cloud. Seguono lo stesso esempio diversi modelli di risposta agli incidenti che supportano questi principi di sicurezza, tra cui la conservazione dei log, la selezione degli avvisi derivata dalla modellazione delle minacce, lo sviluppo di playbook e l'integrazione della gestione delle informazioni e degli eventi di sicurezza (SIEM). Le differenze iniziano quando i clienti iniziano a progettare e progettare questi modelli nel cloud. Di seguito sono riportate le principali differenze nella risposta agli incidenti in AWS.

Differenza #1: La sicurezza come responsabilità condivisa

La responsabilità per la sicurezza e la conformità è condivisa tra AWS e i suoi clienti. Questo modello di responsabilità condivisa allevia parte dell'onere operativo del cliente perché AWS gestisce, gestisce e controlla i componenti, dal sistema operativo host e dal livello di virtualizzazione fino alla sicurezza fisica delle strutture in cui opera il servizio. Per maggiori dettagli sul modello di responsabilità condivisa, consulta la documentazione del modello di [responsabilità condivisa](#).

Man mano che la responsabilità condivisa nel cloud cambia, cambiano anche le opzioni di risposta agli incidenti. Pianificare e comprendere questi compromessi e abbinarli alle esigenze di governance è un passaggio fondamentale nella risposta agli incidenti.

Oltre alla relazione diretta con cui avete AWS, potrebbero esserci altre entità che hanno responsabilità nel vostro particolare modello di responsabilità. Ad esempio, potreste avere unità organizzative interne che si assumono la responsabilità di alcuni aspetti delle vostre operazioni. Potreste anche avere rapporti con altre parti che sviluppano, gestiscono o gestiscono parte della vostra tecnologia cloud.

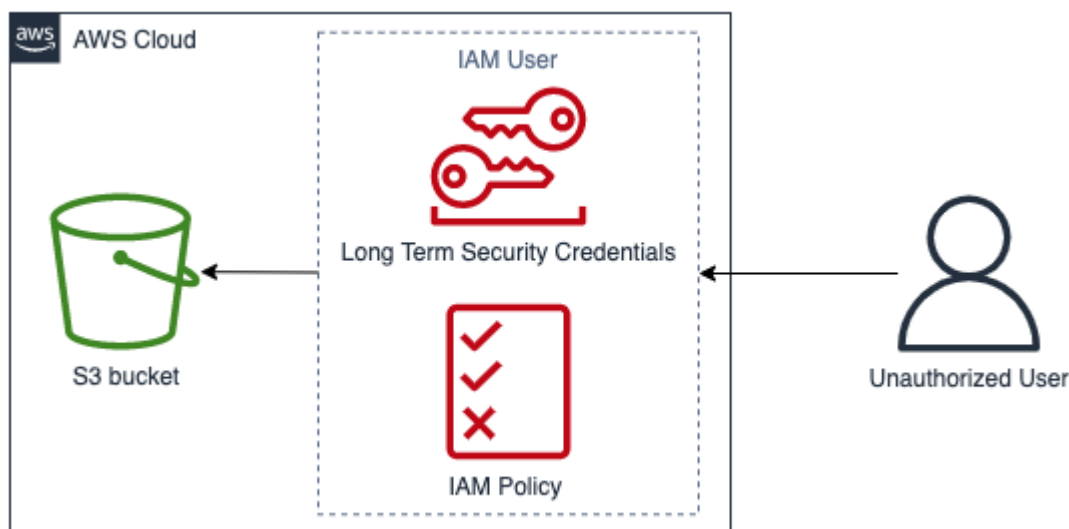
È estremamente importante creare e testare un piano di risposta agli incidenti appropriato e playbook appropriati che corrispondano al modello operativo in uso.

Differenza #2: dominio del servizio cloud

A causa delle differenze di responsabilità in materia di sicurezza esistenti nei servizi cloud, è stato introdotto un nuovo dominio per gli incidenti di sicurezza: il dominio dei servizi, che è stato spiegato in precedenza nella sezione [Dominio degli incidenti](#). Il dominio del servizio comprende l' AWS account del cliente, le autorizzazioni IAM, i metadati delle risorse, la fatturazione e altre aree. Questo dominio è diverso per quanto riguarda la risposta agli incidenti a causa del modo in cui rispondi. La risposta

all'interno del dominio del servizio viene in genere effettuata esaminando ed emettendo chiamate API, anziché una risposta tradizionale basata su host e rete. Nel dominio del servizio, non interagisci con il sistema operativo della risorsa interessata.

Il diagramma seguente mostra un esempio di evento di sicurezza nel dominio del servizio basato su un anti-pattern architetturale. In questo caso, un utente non autorizzato ottiene le credenziali di sicurezza a lungo termine di un utente IAM. L'utente IAM dispone di una policy IAM che gli consente di recuperare oggetti da un bucket [Amazon Simple Storage Service](#) (Amazon S3). Per rispondere a questo evento di sicurezza, dovresti AWS APIs analizzare AWS log come i log di accesso [AWS CloudTrail](#) di Amazon S3. È inoltre possibile AWS APIs utilizzarlo per contenere l'incidente e recuperarlo.



Esempio di dominio di servizio

Differenza #3: APIs per il provisioning dell'infrastruttura

Un'altra differenza deriva dalla [caratteristica cloud del self-service on-demand](#). La struttura principale con cui i clienti interagiscono Cloud AWS utilizzando un' RESTful API tramite endpoint pubblici e privati disponibili in molte aree geografiche in tutto il mondo. I clienti possono accedere a questi endpoint API con AWS credenziali. A differenza del controllo di accesso locale, queste credenziali non sono necessariamente vincolate da una rete o da un dominio Microsoft Active Directory. Le credenziali sono invece associate a un principale IAM all'interno di un account. AWS È possibile accedere a questi endpoint API al di fuori della rete aziendale, un aspetto importante da comprendere quando si risponde a un incidente in cui le credenziali vengono utilizzate al di fuori della rete o dell'area geografica prevista.

Data la natura basata su API di AWS, un'importante fonte di log per rispondere agli eventi di sicurezza è AWS CloudTrail quella che tiene traccia delle chiamate API di gestione effettuate negli AWS account e dove è possibile trovare informazioni sulla posizione di origine delle chiamate API.

Differenza #4: natura dinamica del cloud

Il cloud è dinamico e consente di creare ed eliminare rapidamente risorse. Con il ridimensionamento automatico, le risorse possono essere aumentate e ridotte in base all'aumento del traffico. Con un'infrastruttura di breve durata e cambiamenti rapidi, una risorsa su cui stai indagando potrebbe non esistere più o potrebbe essere stata modificata. Comprendere la natura effimera delle AWS risorse e come monitorare la creazione e l'eliminazione delle risorse sarà importante per l'analisi degli AWS incidenti. È possibile utilizzarlo [AWS Config](#) per tenere traccia della cronologia di configurazione delle risorse. AWS

Differenza #5: accesso ai dati

Anche l'accesso ai dati è diverso nel cloud. Non è possibile collegarsi a un server per raccogliere i dati necessari per un'indagine di sicurezza. I dati vengono raccolti via cavo e tramite chiamate API. Dovrai esercitarti e capire come eseguire nuovamente la raccolta dei dati per prepararti a questo cambiamento e verificare l'archiviazione appropriata per una raccolta e un accesso efficaci. APIs

Differenza #6: importanza dell'automazione

Affinché i clienti possano sfruttare appieno i vantaggi dell'adozione del cloud, la loro strategia operativa deve abbracciare l'automazione. L'infrastruttura come codice (IaC) è un modello di ambienti automatizzati altamente efficienti in cui AWS i servizi vengono distribuiti, configurati, riconfigurati e distrutti utilizzando il codice facilitato da servizi IaC nativi come o soluzioni di terze parti. [AWS CloudFormation](#) Ciò spinge l'implementazione della risposta agli incidenti a essere altamente automatizzata, il che è auspicabile per evitare errori umani, specialmente nella gestione delle prove. Sebbene l'automazione venga utilizzata in sede, è essenziale e più semplice in. Cloud AWS

Risolvere queste differenze

Per risolvere queste differenze, segui i passaggi descritti nella sezione successiva per verificare che il tuo programma di risposta agli incidenti che coinvolga persone, processi e tecnologie sia ben preparato.

Preparazione

Essere preparati per affrontare un incidente è fondamentale per fornire una risposta tempestiva ed efficace. La preparazione viene effettuata in tre ambiti:

- **Persone:** la preparazione del personale a un incidente di sicurezza implica l'identificazione delle parti interessate alla risposta agli incidenti e la loro formazione sulla risposta agli incidenti e sulle tecnologie cloud.
- **Processo:** la preparazione dei processi per un incidente di sicurezza implica la documentazione delle architetture, lo sviluppo di piani di risposta agli incidenti completi e la creazione di playbook per una risposta coerente agli eventi di sicurezza.
- **Tecnologia:** la preparazione della tecnologia per un incidente di sicurezza implica la configurazione dell'accesso, l'aggregazione e il monitoraggio dei registri necessari, l'implementazione di meccanismi di allarme efficaci e lo sviluppo di capacità di risposta e investigative.

Ciascuno di questi domini è importante per una risposta efficace agli imprevisti. Nessun programma di risposta agli imprevisti è completo o efficace senza tutti e tre. Una preparazione agli incidenti può dirsi efficace solo se le persone, i processi e le tecnologie sono stati preparati in maniera adeguata e integrata.

Persone

Per rispondere a un evento di sicurezza, è necessario identificare le parti interessate che potrebbero supportare la risposta a un evento di sicurezza. Inoltre, per una risposta efficace è fondamentale che siano formati sulle AWS tecnologie e sull' AWS ambiente in uso.

Definisci ruoli e responsabilità

La gestione degli eventi di sicurezza richiede disciplina interorganizzativa e propensione all'azione. All'interno della struttura organizzativa, dovrebbero esserci molte persone da considerarsi responsabili, affidabili, consultabili o informate durante un incidente, come i rappresentanti delle risorse umane (HR), i membri del team esecutivo e quelli dell'ufficio legale. Considera questi ruoli e queste responsabilità e, se è necessario, coinvolgi terze parti. Tieni presente che in molte aree geografiche esistono leggi locali che regolano ciò che deve e non deve essere fatto. Sebbene possa sembrare burocratico creare una tabella RACI (responsabile, responsabile, consultata e informata) per i piani di risposta alla sicurezza, ciò consente una comunicazione rapida e diretta e delinea chiaramente la leadership nelle diverse fasi dell'evento.

Durante un incidente, l'inclusione delle applicazioni e owners/developers delle risorse interessate è fondamentale perché si tratta di esperti in materia (SMEs) in grado di fornire informazioni e contesto per aiutare a misurare l'impatto. Assicurati di fare pratica e instaurare relazioni con sviluppatori e proprietari delle applicazioni prima di affidarti alla loro esperienza per la gestione della risposta agli incidenti. I proprietari delle applicazioni o SMEs, ad esempio, gli amministratori o gli ingegneri del

cloud, potrebbero dover agire in situazioni in cui l'ambiente non è familiare o presenta complessità o in cui i soccorritori non hanno accesso.

Infine, nell'indagine o nella risposta potrebbero essere coinvolte relazioni di fiducia perché possono fornire competenze aggiuntive e analisi preziose. Quando non disponi di queste competenze nel tuo team, potresti voler assumere una persona esterna per assistenza.

Formare il personale addetto alla risposta agli

La formazione del personale addetto alla risposta agli incidenti sulle tecnologie utilizzate dall'organizzazione sarà fondamentale per rispondere adeguatamente a un evento di sicurezza. Le risposte potrebbero essere prolungate se i membri dello staff non comprendono le tecnologie di base. Oltre ai tradizionali concetti di risposta agli incidenti, è anche importante che comprendano AWS i servizi e il loro AWS ambiente. Esistono diversi meccanismi tradizionali per la formazione del personale addetto agli incidenti, come la formazione online e la formazione in aula. Come meccanismo di allenamento, dovrete considerare anche la possibilità di organizzare giornate di gioco o simulazioni. Per i dettagli su come eseguire le simulazioni, consulta la [the section called "Esegui simulazioni regolari"](#) sezione di questo documento.

Comprendi le tecnologie Cloud AWS

Per ridurre le dipendenze e ridurre i tempi di risposta, assicurati che i team di sicurezza e i soccorritori siano istruiti sui servizi cloud e abbiano l'opportunità di fare pratica con lo specifico ambiente cloud utilizzato dalla tua organizzazione. Affinché i soccorritori siano efficaci, è importante conoscere AWS le basi, lo IAM AWS Organizations, i servizi di AWS registrazione e monitoraggio e i servizi di sicurezza. AWS

AWS offre workshop sulla sicurezza online (consulta [AWS Security Workshop](#)) in cui è possibile acquisire esperienze pratiche con i servizi di AWS sicurezza e monitoraggio. AWS offre inoltre una serie di opzioni di formazione e percorsi di apprendimento attraverso formazione digitale, formazione in aula, partner di formazione e AWS certificazioni. Per ulteriori informazioni, consulta [AWS Formazione e certificazione](#).

AWS offre corsi di formazione gratuiti e in abbonamento a supporto di più persone e aree di interesse. Visita [AWS Skillbuilder](#) per saperne di più.

Comprendi il tuo ambiente AWS

Oltre a comprendere AWS i servizi, i relativi casi d'uso e il modo in cui si integrano tra loro, è altrettanto importante capire come è effettivamente architettato AWS l'ambiente dell'organizzazione e quali processi operativi sono in atto. Spesso, conoscenze interne come queste non sono

documentate e vengono comprese solo da pochi esperti di settore, il che può creare dipendenze, ostacolare l'innovazione e rallentare i tempi di risposta.

Per evitare queste dipendenze e accelerare i tempi di risposta, la conoscenza interna dell' AWS ambiente deve essere documentata, accessibile e compresa dagli analisti della sicurezza. La comprensione completa dell'impronta del cloud richiederà la collaborazione tra le parti interessate alla sicurezza e gli amministratori del cloud. Parte della preparazione dei processi per la risposta agli incidenti include la documentazione e la centralizzazione dei diagrammi di architettura, come illustrato più avanti in questo white paper. [the section called “Documenta e centralizza i diagrammi di architettura”](#) Tuttavia, dal punto di vista delle persone, è importante che gli analisti possano accedere e comprendere i diagrammi e i processi operativi relativi all'ambiente in uso. AWS

Comprendi i team di AWS risposta e il supporto

Supporto

[Supporto](#) offre una gamma di piani che forniscono l'accesso a strumenti e competenze che supportano il successo e lo stato operativo delle vostre AWS soluzioni. Se avete bisogno di supporto tecnico e di ulteriori risorse per pianificare, implementare e ottimizzare AWS l'ambiente, potete selezionare il piano di supporto più adatto al vostro caso AWS d'uso.

Considera il [Support Center](#) di Console di gestione AWS (è richiesto l'accesso) come punto di contatto centrale per ricevere assistenza per problemi che riguardano AWS le tue risorse. L'accesso a Supporto è controllato da IAM. Per ulteriori informazioni su come accedere alle funzionalità di AWS Support, consulta [Guida introduttiva Supporto](#).

Inoltre, se devi segnalare un abuso, contatta il [team di AWS Trust and Safety](#).

Ingegneri della sicurezza in caso di incidente

I tecnici di Security Incident Response sono un AWS team globale specializzato e sempre disponibile che fornisce supporto ai clienti durante gli eventi di sicurezza attivi dal punto di vista del cliente nell'ambito del [Modello di responsabilitàAWS condivisa](#).

Quando i tecnici di Security Incident Response ti supportano, riceverai assistenza per la valutazione e il ripristino in caso di evento di sicurezza attivo. AWS Vi assisteranno nell'analisi delle cause principali attraverso l'uso dei log di AWS servizio e vi forniranno consigli per il ripristino. Forniranno inoltre consigli sulla sicurezza e best practice per aiutarti a evitare eventi di sicurezza in futuro.

AWS i clienti possono contattare i tecnici del Security Incident Response tramite un [caso di AWS supporto](#).

- Tutti i clienti:
 1. Account e fatturazione
 2. Servizio: Account
 3. Categoria: Sicurezza
 4. Gravità: domanda generale
- Clienti con Supporto piani Developer:
 1. Account e fatturazione
 2. Servizio: Account
 3. Categoria: Sicurezza
 4. Severità: domanda importante
- Clienti con Supporto piani aziendali:
 1. Account e fatturazione
 2. Servizio: Account
 3. Categoria: Sicurezza
 4. Severità: domanda urgente che ha un impatto sull'attività
- Clienti con Supporto piani Enterprise:
 1. Account e fatturazione
 2. Servizio: Account
 3. Categoria: Sicurezza
 4. Severità: domanda critica sul rischio aziendale
- Clienti con AWS Security Incident Response abbonamenti: aprire la console Security Incident Response all'indirizzo <https://console.aws.amazon.com/security-ir/>

DDoSupporto di risposta S

AWS offre [AWS Shield](#), che fornisce un servizio di protezione gestito dalla denial of service (DDoS) distribuito che salvaguarda le applicazioni Web in esecuzione su. AWS AWS Shield fornisce un ~~rilevamento sempre attivo e mitigazioni automatiche in linea in grado di ridurre al minimo i tempi di~~

inattività e la latenza delle applicazioni, quindi non è necessario impegnarsi per trarre vantaggio dalla protezione S. Supporto DDo Esistono due livelli di AWS Shield: Shield Standard e Shield Advanced. Per ulteriori informazioni sulle differenze tra questi due livelli, consulta la [documentazione sulle funzionalità di Shield](#).

AWS Managed Services (AMS)

[AWS Managed Services](#)(AMS) offre una gestione continua dell' AWS infrastruttura in modo che possiate concentrarvi sulle vostre applicazioni. Grazie all'implementazione di best practice per la manutenzione dell'infrastruttura, AMS consente di ridurre rischi e costi operativi. AMS automatizza attività frequenti quali richieste di modifica, monitoraggio, gestione di patch, sicurezza e backup, nonché fornisce servizi completi per il ciclo di vita per gestire provisioning, esecuzione e supporto dell'infrastruttura.

AMS si assume la responsabilità di implementare una suite di controlli di sicurezza e fornisce ogni giorno una prima linea di risposta agli avvisi. In caso di avviso, AMS si attiene a una serie standard di playbook automatici e manuali per verificare una risposta coerente. Questi playbook vengono condivisi con i clienti AMS durante l'onboarding in modo che possano sviluppare e coordinare una risposta con AMS.

Processo

Lo sviluppo di processi di risposta agli incidenti completi e chiaramente definiti è fondamentale per un programma di risposta agli incidenti efficace e scalabile. Quando si verifica un evento di sicurezza, procedure e flussi di lavoro chiari vi aiuteranno a rispondere in modo tempestivo. È possibile che esistano già dei processi di risposta agli incidenti. Indipendentemente dallo stato attuale, è importante aggiornare, iterare e testare con regolarità i processi di risposta agli incidenti.

Sviluppa e testa un piano di risposta agli incidenti

Il primo documento da sviluppare per la risposta agli incidenti è il piano di risposta agli incidenti. Lo scopo del piano di risposta agli incidenti è costituire la base del programma e della strategia di risposta agli incidenti. Un piano di risposta agli incidenti è un documento di alto livello che in genere include le seguenti sezioni:

- **Panoramica del team di risposta agli incidenti:** delinea gli obiettivi e le funzioni del team di risposta agli incidenti
- **Ruoli e responsabilità:** elenca le parti interessate alla risposta agli incidenti e descrive in dettaglio i loro ruoli quando si verifica un incidente

- Un piano di comunicazione: descrive in dettaglio le informazioni di contatto e il modo in cui comunicherai durante un incidente

È consigliabile utilizzare la out-of-band comunicazione come supporto per la comunicazione in caso di incidente. Un esempio di applicazione che fornisce un canale di out-of-band comunicazione sicuro è [AWS Wickr](#).

- Fasi di risposta agli incidenti e azioni da intraprendere: enumera le fasi di risposta agli incidenti, ad esempio rilevamento, analisi, eliminazione, contenimento e ripristino, comprese le azioni di alto livello da intraprendere nell'ambito di tali fasi
- Definizioni di gravità e prioritizzazione degli incidenti: descrive in dettaglio come classificare la gravità di un incidente, come assegnare priorità all'incidente e quindi in che modo le definizioni di gravità influiscono sulle procedure di escalation

Sebbene queste sezioni siano comuni ad aziende di diverse dimensioni e settori, il piano di risposta agli incidenti di ciascuna organizzazione è unico. Dovrai creare un piano di risposta agli incidenti che funzioni meglio per la tua organizzazione.

Documenta e centralizza i diagrammi di architettura

Per rispondere in modo rapido e preciso a un evento di sicurezza, è necessario comprendere come sono architettati i sistemi e le reti. La comprensione di questi modelli interni non è importante solo per la risposta agli incidenti, ma anche per verificare la coerenza tra le applicazioni con cui sono progettati i modelli, secondo le migliori pratiche. È inoltre necessario verificare che questa documentazione sia aggiornata e regolarmente aggiornata in base ai nuovi modelli di architettura. È necessario sviluppare documentazione e archivi interni che descrivano in dettaglio elementi come:

- AWS struttura dell'account - Devi sapere:
 - Quanti AWS account hai?
 - Come sono organizzati questi AWS conti?
 - Chi sono i titolari aziendali degli AWS account?
 - Utilizzate Service Control Policies (SCPs)? In caso affermativo, quali barriere organizzative vengono implementate utilizzando? SCPs
 - Sono previste limitazioni alle regioni e ai servizi che è possibile utilizzare?
 - Quali sono le differenze tra le unità aziendali e gli ambienti (dev/test/prod)?
- AWS modelli di servizio
 - Quali AWS servizi utilizzi?

- Quali sono i AWS servizi più utilizzati?
- Modelli di architettura
 - Quali architetture cloud utilizzate?
- AWS modelli di autenticazione
 - In che modo i tuoi sviluppatori si autenticano in genere? AWS
 - Utilizzate ruoli o utenti IAM (o entrambi)? La tua autenticazione è AWS connessa a un provider di identità (IdP)?
 - Come si fa a mappare un ruolo o un utente IAM a un dipendente o a un sistema?
 - In che modo l'accesso viene revocato quando qualcuno non è più autorizzato?
- AWS modelli di autorizzazione
 - Quali politiche IAM utilizzano i tuoi sviluppatori?
 - Utilizzate politiche basate sulle risorse?
- Registrazione e monitoraggio
 - Quali fonti di registrazione utilizzate e dove vengono archiviate?
 - Aggregate AWS CloudTrail i log? In caso affermativo, dove vengono archiviati?
 - Come si interrogano CloudTrail i log?
 - Hai GuardDuty abilitato Amazon?
 - Come si accede ai GuardDuty risultati (ad esempio, console, sistema di ticketing, SIEM)?
 - I risultati o gli eventi sono aggregati in un SIEM?
 - I biglietti vengono creati automaticamente?
 - Quali strumenti sono disponibili per analizzare i registri per un'indagine?
- Topologia di rete
 - Come sono disposti fisicamente o logicamente i dispositivi, gli endpoint e le connessioni della rete?
 - Come si connette la tua rete a? AWS
 - Come viene filtrato il traffico di rete tra gli ambienti?
- Infrastruttura esterna
 - Come vengono implementate le applicazioni rivolte verso l'esterno?
 - Quali risorse sono accessibili AWS al pubblico?
 - Quali AWS account contengono un'infrastruttura rivolta verso l'esterno?

La documentazione dei diagrammi e dei processi tecnici interni facilita il lavoro dell'analista di risposta agli incidenti, aiutandolo ad acquisire rapidamente le conoscenze istituzionali necessarie per rispondere a un evento di sicurezza. Una documentazione completa dei processi tecnici interni non solo semplifica le indagini di sicurezza, ma consente anche la razionalizzazione e la valutazione dei processi.

Sviluppa dei playbook per la risposta agli incidenti

Una parte fondamentale della preparazione dei processi di risposta agli incidenti è costituita dalla predisposizione di playbook. I playbook di risposta agli incidenti forniscono una serie di indicazioni prescrittive e di passaggi da seguire in caso di evento di sicurezza. Una struttura e passaggi chiari semplificano la risposta e riducono la probabilità di errore umano.

Per cosa creare playbook

È necessario creare i playbook per scenari di incidenti come:

- Incidenti previsti: i playbook devono essere creati per gli incidenti che prevedi. tra cui minacce come Denial of Service (DoS), ransomware e la compromissione delle credenziali.
- Rilevamenti o avvisi di sicurezza noti: è necessario creare dei playbook per i risultati e gli avvisi di sicurezza noti, ad esempio i risultati. GuardDuty Potresti ricevere una GuardDuty scoperta e pensare: «E adesso?» Per evitare che una GuardDuty scoperta venga gestita male o che la si ignori, crea un manuale per ogni potenziale scoperta. GuardDuty [Alcuni dettagli e linee guida sulla correzione sono disponibili nella documentazione. GuardDuty](#) Vale la pena notare che non GuardDuty è abilitato di default e comporta un costo. Maggiori dettagli su sono GuardDuty disponibili nell'Appendice A: Definizioni delle funzionalità cloud -. [the section called “Visibilità e avvisi”](#)

Cosa includere nei playbook

I playbook devono contenere i passaggi tecnici che un analista della sicurezza deve seguire per indagare e rispondere in modo adeguato a un potenziale incidente di sicurezza.

Gli elementi da includere in un playbook sono:

- Panoramica del playbook: a quale scenario di rischio o incidente si riferisce questo playbook? Qual è l'obiettivo del playbook?
- Prerequisiti: quali registri e meccanismi di rilevamento sono necessari per questo scenario di incidente? Qual è la notifica prevista?

- Informazioni sulle parti interessate: chi è coinvolto e quali sono le loro informazioni di contatto? Quali sono le responsabilità di ciascuna parte interessata?
- Fasi di risposta: in tutte le fasi della risposta agli incidenti, quali misure tattiche dovrebbero essere adottate? Quali query deve eseguire l'analista? Quale codice va eseguito per ottenere il risultato desiderato?
 - Rileva: come verrà rilevato l'incidente?
 - Analizza: come verrà determinata la portata dell'impatto?
 - Contenere: in che modo verrà isolato l'incidente per limitarne l'ambito?
 - Eradicazione: come verrà rimossa la minaccia dall'ambiente?
 - Ripristino: in che modo il sistema o la risorsa interessati verranno riportati in produzione?
- Risultati attesi: dopo l'esecuzione delle query e del codice, qual è il risultato previsto del playbook?

Per verificare la coerenza delle informazioni in ogni playbook, può essere utile creare un modello di playbook da utilizzare negli altri playbook di sicurezza. Alcuni degli elementi elencati in precedenza, come le informazioni sugli stakeholder, possono essere condivisi tra più playbook. In tal caso, puoi creare una documentazione centralizzata per tali informazioni e farvi riferimento nel playbook, quindi enumerare le differenze esplicite nel playbook. In questo modo eviterai di dover aggiornare le stesse informazioni in tutti i tuoi playbook individuali. Creando un modello e identificando le informazioni comuni o condivise nei playbook, puoi semplificare e velocizzare lo sviluppo dei playbook. Infine, è probabile che i tuoi playbook si evolveranno nel tempo; una volta confermata la coerenza dei passaggi, ecco i requisiti per l'automazione.

Playbook di esempio

Alcuni playbook di esempio sono disponibili nell'Appendice B in [the section called “Risorse del playbook”](#). Gli esempi riportati di seguito possono essere utilizzati per guidarvi su quali playbook creare e cosa includere nei playbook. Tuttavia, è importante creare dei playbook che includano i rischi più rilevanti per la tua attività. Devi verificare che i passaggi e i flussi di lavoro all'interno dei tuoi playbook includano le tue tecnologie e i tuoi processi.

Esegui simulazioni regolari

Le organizzazioni crescono e si evolvono nel tempo, così come il panorama delle minacce. Per questo motivo, è importante rivedere continuamente le proprie capacità di risposta agli incidenti. Le simulazioni sono un metodo che può essere utilizzato per eseguire questa valutazione. Le simulazioni utilizzano scenari di eventi di sicurezza reali progettati per imitare le tattiche, le tecniche e le procedure di un autore della minaccia (TTPs) e consentono a un'organizzazione di esercitare e

valutare le proprie capacità di risposta agli incidenti rispondendo a questi finti eventi informatici così come potrebbero verificarsi nella realtà.

Le simulazioni offrono una serie di vantaggi, tra cui:

- Convalida della preparazione informatica e sviluppo della fiducia dei team di risposta agli incidenti.
- Verifica della precisione e dell'efficienza di strumenti e flussi di lavoro.
- Perfezionamento dei metodi di comunicazione ed escalation in linea con il piano di risposta agli incidenti.
- Opportunità di rispondere per i vettori meno comuni.

Tipi di simulazioni

Esistono tre tipi principali di simulazioni:

- **Esercizi da tavolo:** l'approccio da tavolo alle simulazioni è strettamente una sessione basata sulla discussione che coinvolge le varie parti interessate alla risposta agli incidenti per mettere in pratica ruoli e responsabilità e utilizzare strumenti di comunicazione e playbook consolidati. La facilitazione dell'esercizio in genere può essere eseguita in un'intera giornata in un luogo virtuale, fisico o in una combinazione di essi. A causa della sua natura basata sulla discussione, l'esercizio da tavolo si concentra su processi, persone e collaborazione. La tecnologia è parte integrante della discussione; tuttavia, l'uso effettivo di strumenti o script di risposta agli incidenti in genere non rientra nell'esercizio da tavolo.
- **Esercizi Purple Team:** gli esercizi Purple Team aumentano il livello di collaborazione tra i soccorritori (Blue Team) e gli attori simulati delle minacce (Red Team). Il Blue Team è generalmente composto da membri del Security Operations Center (SOC), ma può includere anche altre parti interessate che potrebbero essere coinvolte durante un vero evento informatico. Il Red Team è generalmente composto da un team di test di penetrazione o da stakeholder chiave formati in materia di sicurezza offensiva. Il Red Team collabora con i facilitatori degli esercizi durante la progettazione di uno scenario in modo che lo scenario sia accurato e fattibile. Durante le esercitazioni del Purple Team, l'attenzione principale è rivolta ai meccanismi di rilevamento, agli strumenti e alle procedure operative standard (SOPs) a supporto degli sforzi di risposta agli incidenti.
- **Esercizi della Squadra Rossa** — Durante un'esercitazione della Squadra Rossa, l'attacco (Squadra Rossa) conduce una simulazione per raggiungere un determinato obiettivo o una serie di obiettivi da un ambito predeterminato. I difensori (Blue Team) non necessariamente conosceranno la portata e la durata dell'esercitazione, il che fornisce una valutazione più realistica di come

reagirebbero a un incidente reale. Poiché gli esercizi della Red Team possono essere test invasivi, è necessario prestare attenzione e implementare controlli per verificare che l'esercizio non provochi danni effettivi all'ambiente.

Note

AWS richiede ai clienti di rivedere la politica per i test di penetrazione disponibile sul [sito web di Penetration Testing](#) prima di condurre gli esercizi del Purple Team o del Red Team.

La Tabella 1 riassume alcune differenze chiave in questi tipi di simulazioni. È importante notare che le definizioni sono generalmente considerate generiche e possono essere personalizzate per soddisfare le esigenze dell'organizzazione.

Tabella 1 — Tipi di simulazioni

	Esercizio da tavolo	Esercizio Purple Team	Esercizio della squadra rossa
Riepilogo	Esercizi cartacei incentrati su uno specifico scenario di incidente di sicurezza. Questi possono essere di alto livello o tecnici e sono azionati da una serie di iniezioni di carta.	Un'offerta più realistica a rispetto agli esercizi da tavolo. Durante gli esercizi del Purple Team, i facilitatori collaborano con i partecipanti per aumentare il coinvolgimento negli esercizi e offrire formazione laddove necessario.	Generalmente un'offerta di simulazione più avanzata. Di solito c'è un alto livello di segretezza, in cui i partecipanti potrebbero non conoscere tutti i dettagli dell'esercizio.
Risorse richieste	Risorse tecniche limitate richieste	Sono necessarie diverse parti interessate e un elevato livello di risorse tecniche	Sono necessarie diverse parti interessate e sono necessarie risorse tecniche di alto livello
Complessità	Bassa	Media	Elevata

Prendi in considerazione la possibilità di svolgere simulazioni informatiche a intervalli regolari. Ogni tipo di esercizio può offrire vantaggi unici ai partecipanti e all'organizzazione nel suo insieme, quindi potresti scegliere di iniziare con tipi di simulazione meno complessi (come gli esercizi da tavolo) e passare a tipi di simulazione più complessi (esercizi della Squadra Rossa). È necessario selezionare un tipo di simulazione in base alla maturità, alle risorse e ai risultati desiderati a livello di sicurezza. Alcuni clienti potrebbero non scegliere di eseguire gli esercizi del Red Team a causa della complessità e dei costi.

Ciclo di vita dell'esercizio

Indipendentemente dal tipo di simulazione scelto, le simulazioni generalmente seguono questi passaggi:

1. Definisci gli elementi principali dell'esercizio: definisci lo scenario di simulazione e gli obiettivi della simulazione. Lo scenario e gli obiettivi dovrebbero essere entrambi accettati dalla leadership.
2. Identifica le principali parti interessate: come minimo, un'esercitazione necessita di facilitatori e partecipanti all'esercizio. A seconda dello scenario, potrebbero essere coinvolte altre parti interessate come la leadership legale, delle comunicazioni o esecutiva.
3. Crea e testa lo scenario: potrebbe essere necessario ridefinire lo scenario in fase di creazione se elementi specifici non sono fattibili. Come risultato di questa fase è previsto uno scenario definitivo.
4. Facilitare la simulazione: il tipo di simulazione determina la facilitazione utilizzata (scenario cartaceo rispetto a uno scenario simulato altamente tecnico). I coordinatori dovrebbero allineare le loro tattiche di svolgimento agli oggetti dell'esercitazione e dovrebbero coinvolgere tutti i partecipanti ove possibile per ottimizzare i benefici.
5. Sviluppa il rapporto post-azione (AAR): identifica le aree che sono andate bene, quelle che possono essere migliorate e le potenziali lacune. Il report AAR dovrebbe misurare l'efficacia della simulazione e la risposta del team all'evento simulato in modo che i progressi possano essere monitorati nel tempo con simulazioni future.

Tecnologia

Se sviluppate e implementate le tecnologie appropriate prima di un incidente di sicurezza, il personale addetto alla risposta agli incidenti sarà in grado di indagare, comprenderne l'ambito e agire tempestivamente.

Sviluppa la struttura AWS degli account

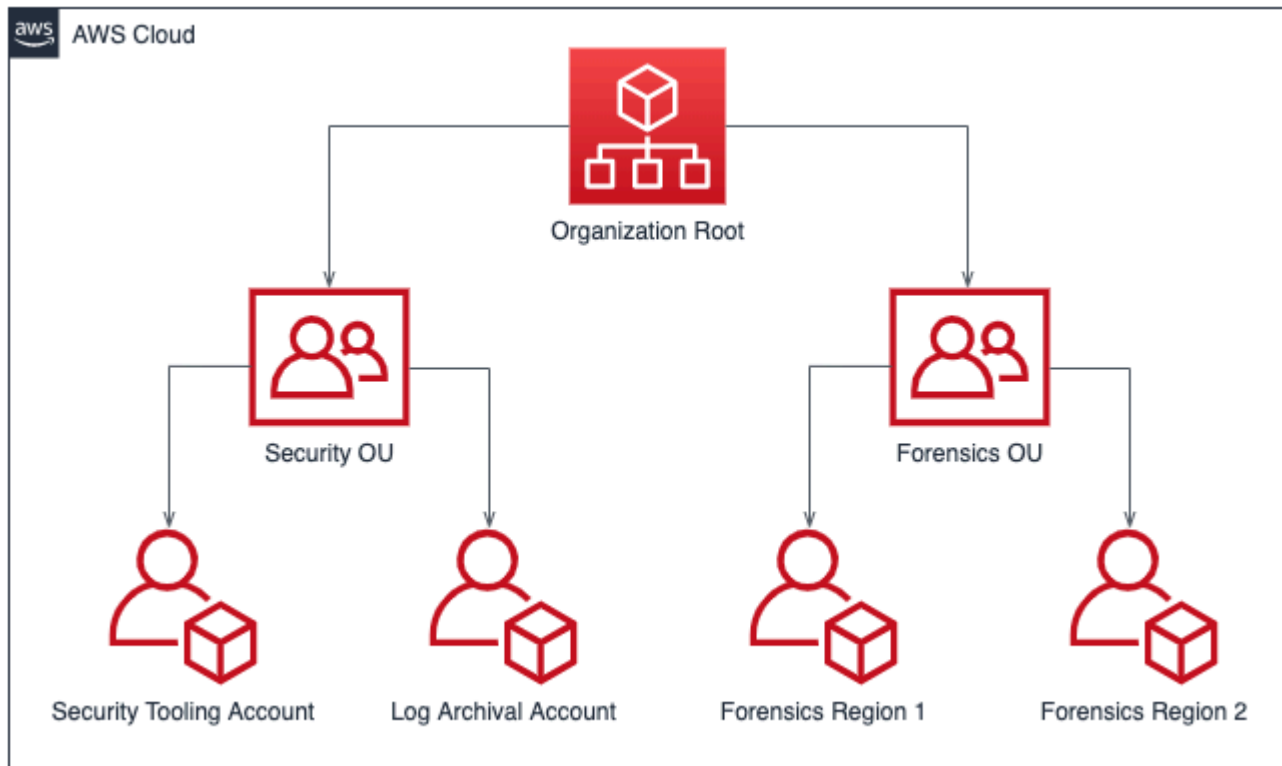
[AWS Organizations](#) aiuta a gestire e governare centralmente un AWS ambiente man mano che si aumentano e si scalano AWS le risorse. Un' AWS organizzazione consolida AWS gli account in modo da poterli amministrare come un'unica unità. È possibile utilizzare le unità organizzative (OUs) per raggruppare gli account e amministrarli come un'unica unità.

Per la risposta agli incidenti, è utile disporre di una struttura di AWS account che supporti le funzioni di risposta agli incidenti, che includa un'unità organizzativa di sicurezza e un'unità organizzativa forense. All'interno dell'unità organizzativa di sicurezza, è necessario disporre degli account per:

- Archiviazione dei log: aggrega i log in un account di archiviazione dei log. AWS
- Strumenti di sicurezza: centralizza i servizi di sicurezza in un account dello strumento di sicurezza. AWS Questo account funge da amministratore delegato per i servizi di sicurezza.

Nell'unità organizzativa con funzionalità forensi, puoi implementare uno o più account con funzionalità forensi per ciascuna regione in cui operi, a seconda di quale è più adatta all'azienda e al modello operativo. Per un esempio di approccio basato sull'account per regione, se operi solo negli Stati Uniti orientali (Virginia settentrionale) (us-east-1) e negli Stati Uniti occidentali (Oregon) (us-west-2), allora avresti due account nell'unità organizzativa forensics: uno per us-east-1 e uno per us-west-2. Poiché la creazione di nuovi account richiede tempo, è fondamentale creare e fornire gli strumenti adatti agli account con funzionalità forensi con largo anticipo rispetto agli incidenti, in modo che gli addetti siano preparati a utilizzarli in modo efficace per la risposta.

Il diagramma seguente mostra una struttura degli account di esempio che include un'unità organizzativa con funzionalità forensi con account con funzionalità forensi per regione:



Struttura degli account per regione per la risposta agli incidenti

Svilupa e implementa una strategia di assegnazione tag

Ottenere informazioni contestuali sul caso d'uso aziendale e sugli stakeholder interni pertinenti che circondano una AWS risorsa può essere difficile. Un modo per farlo è utilizzare i tag, che assegnano metadati alle AWS risorse e sono costituiti da una chiave e un valore definiti dall'utente. Puoi creare i tag per classificare le risorse per scopo, proprietario, ambiente, tipo di dati elaborati e altri criteri di tua scelta.

Una strategia di tagging coerente può velocizzare i tempi di risposta, poiché consente di identificare e distinguere rapidamente le informazioni contestuali su una risorsa. AWS I tag possono anche fungere da meccanismo per avviare le automazioni di risposta. Per ulteriori informazioni su cosa taggare, consulta la [documentazione sull'etichettatura delle risorse](#). AWS Dovrai prima definire i tag nella tua organizzazione e quindi implementare e applicare questa strategia di tag. I dettagli sull'implementazione e l'applicazione sono disponibili nel AWS blog [Implementare la strategia di etichettatura AWS delle risorse utilizzando le politiche di AWS tag e le politiche di controllo dei servizi \(\) SCPs](#).

Aggiorna le informazioni di contatto AWS dell'account

Per ciascuno dei tuoi AWS account, è importante disporre di informazioni di up-to-date contatto accurate in modo che le parti interessate corrette ricevano notifiche importanti AWS su argomenti come sicurezza, fatturazione e operazioni. Per ogni AWS account, hai un contatto principale e contatti alternativi per la sicurezza, la fatturazione e le operazioni. Le differenze tra questi contatti sono riportate nella Guida di [riferimento per la gestione degli AWS account](#).

Per i dettagli sulla gestione dei contatti alternativi, consulta la [AWS documentazione sull'aggiunta, la modifica o la rimozione di contatti alternativi](#). È consigliabile utilizzare una lista di distribuzione e-mail se il team gestisce la fatturazione, le operazioni e i problemi relativi alla sicurezza. Una lista di distribuzione delle e-mail rimuove le dipendenze da una persona, il che può causare blocchi se questa non è in ufficio o lascia l'azienda. È inoltre necessario verificare che l'e-mail e le informazioni di contatto dell'account, incluso il numero di telefono, siano ben protette per difendersi dalla reimpostazione della password dell'account root e dalla reimpostazione dell'autenticazione a più fattori (MFA).

Per i clienti che lo utilizzano AWS Organizations, gli amministratori dell'organizzazione possono gestire centralmente i contatti alternativi per gli account dei membri utilizzando l'account di gestione o un account amministratore delegato senza richiedere credenziali per ogni account. AWS Dovrai inoltre verificare che gli account appena creati contengano informazioni di contatto accurate. Consulta la sezione [Aggiorna automaticamente i contatti alternativi per i post di Account AWS blog appena creati](#).

Prepara l'accesso a Account AWS

Durante un incidente, i team di risposta agli incidenti devono avere accesso agli ambienti e alle risorse coinvolte nell'incidente. Assicurati che i tuoi team abbiano l'accesso appropriato per svolgere le proprie mansioni prima che si verifichi un evento. A tal fine, è necessario conoscere il livello di accesso richiesto dai membri del team (ad esempio, il tipo di azioni che è probabile che intraprendano) e fornire in anticipo l'accesso con il minimo privilegio.

Per implementare e fornire questo accesso, è necessario identificare e discutere la strategia dell' AWS account e la strategia di identità cloud con gli architetti cloud dell'organizzazione per comprendere quali metodi di autenticazione e autorizzazione sono configurati. A causa della natura privilegiata di queste credenziali, è consigliabile prendere in considerazione l'utilizzo dei flussi di approvazione o il recupero delle credenziali da un deposito o da una cassaforte come parte dell'implementazione. Dopo l'implementazione, è necessario documentare e testare l'accesso dei

membri del team ben prima che si verifichi un evento, per assicurarsi che possano rispondere senza ritardi.

Infine, gli utenti creati appositamente per rispondere a un incidente di sicurezza sono spesso privilegiati per fornire un accesso sufficiente. Pertanto, l'uso di queste credenziali deve essere limitato, monitorato e non utilizzato per le attività quotidiane.

Comprendi il panorama delle minacce

Sviluppa modelli di minaccia

Sviluppando modelli di minaccia, le organizzazioni possono identificare le minacce e le mitigazioni prima che lo faccia un utente non autorizzato. Esistono diverse strategie e approcci alla modellazione delle minacce; consulta il post sul blog [How to approach threat modeling](#). Per quanto riguarda la risposta agli incidenti, un modello di minaccia può aiutare a identificare i vettori di attacco che un autore della minaccia potrebbe aver utilizzato durante un incidente. Capire da cosa ti stai difendendo sarà fondamentale per rispondere in modo tempestivo. Puoi anche usare un AWS Partner per la modellazione delle minacce. Per cercare un AWS partner, usa il [AWS Partner Network](#).

Integra e utilizza l'intelligence sulle minacce informatiche

L'intelligence sulle minacce informatiche è costituita dai dati e dall'analisi delle intenzioni, delle opportunità e delle capacità di un autore della minaccia. Ottenere e utilizzare l'intelligence sulle minacce è utile per rilevare tempestivamente un incidente e comprendere meglio il comportamento degli autori delle minacce. L'intelligence sulle minacce informatiche include indicatori statici come indirizzi IP o hash di file di malware. Include anche informazioni di alto livello, come modelli comportamentali e intenti. Puoi raccogliere informazioni sulle minacce da diversi fornitori di sicurezza informatica e da archivi open source.

Per integrare e massimizzare l'intelligence sulle minacce per il proprio AWS ambiente, è possibile utilizzare alcune out-of-the-box funzionalità e integrare elenchi personalizzati di intelligence sulle minacce. Amazon GuardDuty utilizza fonti di intelligence sulle minacce AWS interne e di terze parti. Anche altri AWS servizi, come il firewall DNS e AWS WAF le regole, ricevono input dall' AWS Advanced Threat Intelligence Group. Alcuni GuardDuty risultati vengono mappati nel [MITRE ATT&CK Framework](#), che fornisce informazioni sulle osservazioni del mondo reale sulle tattiche e le tecniche degli avversari.

Seleziona e configura i log per analisi e avvisi

Durante un'indagine di sicurezza, devi essere in grado di esaminare i log pertinenti per registrare e comprendere l'intera portata e la tempistica dell'incidente. I log servono anche per la generazione

di avvisi, che indicano il verificarsi di determinate azioni di interesse. È fondamentale selezionare, attivare, memorizzare e impostare i meccanismi di query e recupero e impostare gli avvisi. Ciascuna di queste azioni viene esaminata in questa sezione. Per maggiori dettagli, consulta il post sul AWS blog [Logging strategies for security incident response](#).

Seleziona e abilita le fonti di registro

Prima di un'indagine di sicurezza, è necessario acquisire i registri pertinenti per ricostruire retroattivamente l'attività di un account. AWS Seleziona e abilita le fonti di registro pertinenti ai carichi di lavoro dei rispettivi account. AWS

AWS CloudTrail è un servizio di registrazione che tiene traccia delle chiamate API effettuate in base all'attività del servizio di acquisizione AWS di un AWS account. È abilitato per impostazione predefinita con una conservazione degli eventi di gestione per 90 giorni che possono essere [recuperati tramite CloudTrail la funzione Event History](#) utilizzando Console di gestione AWS, o un SDK. AWS CLI AWS Per una conservazione e una visibilità più lunghe degli eventi relativi ai dati, è necessario [creare un CloudTrail Trail](#) e associarlo a un bucket Amazon S3 e, facoltativamente, a un gruppo di log. CloudWatch In alternativa, puoi creare un [CloudTrail Lake](#), che conserva CloudTrail i log per un massimo di sette anni e fornisce una funzionalità di interrogazione basata su SQL.

AWS consiglia ai clienti che utilizzano un VPC di abilitare il traffico di rete e i log DNS utilizzando, rispettivamente, [VPC Flow Logs](#) e i log delle [query del resolver Amazon Route 53](#), trasmettendoli in streaming su un bucket Amazon S3 o un gruppo di log. CloudWatch È possibile creare un log di flusso VPC per un VPC, una sottorete o un'interfaccia di rete. Per i log di flusso VPC, puoi scegliere in modo selettivo come e dove abilitare i log di flusso per ridurre i costi.

AWS CloudTrail I log, i log di flusso VPC e i log delle query del resolver Route 53 sono i tre elementi di registrazione di base per supportare le indagini di sicurezza. AWS

AWS i servizi possono generare log non acquisiti dalla tripletta di registrazione di base, ad esempio log di Elastic Load Balancing, log, log del registratore, risultati di Amazon AWS WAF , log di controllo di AWS Config Amazon Elastic GuardDuty Kubernetes Service (Amazon EKS) e log delle applicazioni e del sistema operativo delle istanze Amazon EC2. Per l'elenco completo delle opzioni di registrazione e monitoraggio, consulta [the section called "Appendice A: Definizioni delle funzionalità cloud"](#)

Seleziona l'archiviazione dei registri

La scelta dell'archiviazione dei log è generalmente correlata allo strumento di interrogazione utilizzato, alle capacità di conservazione, alla familiarità e al costo. Quando abiliti i log AWS di

servizio, fornisci una struttura di storage, in genere un bucket CloudWatch o un gruppo di log Amazon S3.

Un bucket Amazon S3 offre uno storage durevole e conveniente con una politica del ciclo di vita opzionale. I log archiviati nei bucket Amazon S3 possono essere interrogati nativamente utilizzando servizi come Amazon Athena. Un gruppo di CloudWatch log fornisce uno storage durevole e una funzione di interrogazione integrata tramite Logs Insights. CloudWatch

Identifica la conservazione dei log appropriata

Quando si utilizza un bucket o un gruppo di CloudWatch log S3 per archiviare i log, è necessario stabilire cicli di vita adeguati per ciascuna fonte di log per ottimizzare i costi di archiviazione e recupero. I clienti dispongono generalmente di log da 3 a 12 mesi a disposizione per l'interrogazione, con una conservazione fino a sette anni. La scelta di disponibilità e conservazione deve essere in linea con i requisiti di sicurezza e con un insieme di mandati statutari, normativi e aziendali.

Seleziona e implementa meccanismi di interrogazione per i log

Nel AWS, i servizi principali che puoi utilizzare per interrogare i log sono [CloudWatch Logs Insights](#) per i dati archiviati in gruppi di CloudWatch log e Amazon [Athena e Amazon Service](#) per i dati archiviati in [OpenSearch Amazon S3](#). Puoi anche utilizzare strumenti di interrogazione di terze parti come SIEM (Security Information and Event Management).

Il processo di selezione di uno strumento di query dei log deve considerare gli aspetti relativi a persone, processi e tecnologia delle operazioni di sicurezza. Scegliete uno strumento che soddisfi i requisiti operativi, aziendali e di sicurezza e che sia accessibile e gestibile a lungo termine. Tieni presente che gli strumenti di query dei log funzionano in modo ottimale quando il numero di log da analizzare è mantenuto entro i limiti dello strumento. Non è raro che i clienti dispongano di più strumenti di interrogazione a causa di vincoli tecnici o di costi. Ad esempio, i clienti potrebbero utilizzare un SIEM di terze parti per eseguire query sugli ultimi 90 giorni di dati e utilizzare Athena per eseguire query oltre i 90 giorni a causa del costo di inserimento dei log di un SIEM. Indipendentemente dall'implementazione, verificate che il vostro approccio riduca al minimo il numero di strumenti necessari per massimizzare l'efficienza operativa, specialmente durante un'indagine su un evento di sicurezza.

Usa i log per avvisare

AWS fornisce avvisi nativamente tramite servizi di sicurezza, come Amazon GuardDuty [AWS Security Hub CSPM](#), e AWS Config. Puoi anche utilizzare motori di generazione di avvisi personalizzati per avvisi di sicurezza non coperti da questi servizi o per avvisi specifici pertinenti al

tuo ambiente. La creazione di questi avvisi e rilevamenti è trattata nella sezione [the section called "Rilevamento"](#) denominata in questo documento.

Sviluppa capacità forensi

Prima che si verifichi un incidente di sicurezza, puoi sviluppare funzionalità forensi per supportare le indagini sugli eventi di sicurezza. La [Guida all'integrazione delle tecniche forensi nella risposta agli incidenti](#) del NIST fornisce tali indicazioni.

Analisi forensi su AWS

Si applicano i concetti della tradizionale analisi forense locale a. AWS Le [strategie relative all'ambiente di indagine forense riportate nel post del Cloud AWS](#) blog forniscono informazioni chiave su cui iniziare a migrare le proprie competenze forensi. AWS

Una volta configurati l'ambiente e la struttura degli AWS account per le indagini forensi, ti consigliamo di definire le tecnologie necessarie per eseguire efficacemente metodologie valide dal punto di vista forense nelle quattro fasi:

- Raccolta: raccogli AWS i log pertinenti, ad esempio i AWS CloudTrail log di flusso VPC e i log a livello di host. AWS Config Raccogli istantanee, backup e dump di memoria delle risorse interessate. AWS
- Esame: esamina i dati raccolti estraendo e valutando le informazioni pertinenti.
- Analisi: analizza i dati raccolti per comprendere l'incidente e trarne conclusioni.
- Segnalazione: presenta le informazioni risultanti dalla fase di analisi.

Acquisizione di backup e snapshot

La configurazione dei backup di sistemi e database importanti è fondamentale per il ripristino da un incidente di sicurezza e per scopi forensi. Grazie ai backup puoi ripristinare i tuoi sistemi allo stato di sicurezza precedente. Su AWS, puoi scattare istantanee di varie risorse. Le istantanee forniscono il point-in-time backup di tali risorse. Esistono molti servizi AWS che offrono supporto nelle operazioni di backup e ripristino. Per informazioni dettagliate su questi servizi [e approcci per il backup e il ripristino, fare riferimento alla Guida prescrittiva](#) per il backup e il ripristino. Per maggiori dettagli, consulta il post sul [blog Use backups to recovery from security incidents](#).

Soprattutto in situazioni come un attacco ransomware, è fondamentale che i backup siano ben protetti. Per indicazioni su come proteggere i backup, consulta le [10 migliori pratiche di sicurezza per proteggere i backup nel](#) post del AWS blog. Oltre a proteggere i backup, è necessario sottoporli

regolarmente a processi di backup e ripristino per verificare che tecnologia e procedure in uso funzionino come previsto.

Automazione delle analisi forensi su AWS

Durante un evento di sicurezza, il team di risposta agli incidenti deve essere in grado di raccogliere e analizzare rapidamente le prove, mantenendo al contempo l'accuratezza per il periodo di tempo che circonda l'evento. Per il team di risposta agli incidenti è sia impegnativo che dispendioso in termini di tempo raccogliere manualmente le prove pertinenti in un ambiente cloud, in particolare su un gran numero di istanze e account. Inoltre, la raccolta manuale può essere soggetta all'errore umano. Per questi motivi, i clienti dovrebbero sviluppare e implementare l'automazione per l'analisi forense.

AWS offre una serie di risorse di automazione per l'analisi forense, che sono consolidate nell'Appendice sotto. [the section called “Risorse forensi”](#) Queste risorse sono esempi di modelli di funzionalità forensi che abbiamo sviluppato, implementate dai clienti. Sebbene costituiscano un'utile architettura di riferimento per iniziare, prendi in considerazione la possibilità di modificarli o creare nuovi modelli di automazione per le funzionalità forensi in base ad ambiente, requisiti, strumenti e processi forensi.

Riepilogo degli elementi di preparazione

Una preparazione accurata per rispondere agli eventi di sicurezza è fondamentale per una risposta tempestiva ed efficace agli incidenti. La preparazione alla risposta agli incidenti coinvolge persone, processi e tecnologia. Tutti e tre questi domini sono ugualmente importanti per la preparazione. È necessario preparare ed evolvere il programma di risposta agli incidenti in tutti e tre i domini.

La Tabella 2 riassume gli elementi di preparazione descritti in questa sezione.

Tabella 2 — Elementi di preparazione della risposta agli incidenti

Dominio	Elemento di preparazione	Elementi d'azione
Persone	Definisci ruoli e responsabilità.	<ul style="list-style-type: none"> Identifica gli stakeholder pertinenti alla risposta agli incidenti. Sviluppa un grafico (RACI) responsabile, responsabile, informato e consultato (RACI) per un incidente.

Dominio	Elemento di preparazione	Elementi d'azione
Persone	Formare il personale addetto alla risposta agli incidenti su AWS.	<ul style="list-style-type: none">• Formare le parti interessate alla risposta agli incidenti sulle AWS basi.• Forma gli stakeholder addetti alla risposta agli incidenti sui servizi di AWS sicurezza e monitoraggio.• Addestra gli stakeholder addetti alla risposta agli incidenti sul tuo AWS ambiente e su come è progettato.
Persone	Comprendi le opzioni di AWS supporto.	<ul style="list-style-type: none">• Comprendi le differenze in termini di AWS supporto, tecnici di Security Incident Response, DDoS response team (DRT) e AMS.• Comprendi il percorso di triage e di escalation per contattare i tecnici del Security Incident Response durante un evento di sicurezza attivo, se necessario.

Dominio	Elemento di preparazione	Elementi d'azione
Processo	Sviluppa un piano di risposta agli incidenti.	<ul style="list-style-type: none"> • Crea un documento di alto livello che definisca il programma e la strategia di risposta agli incidenti. • Includi nel piano di risposta agli incidenti un RACI, un piano di comunicazione, le definizioni degli incidenti e le fasi di risposta agli incidenti.
Processo	Documenta e centralizza i diagrammi di architettura.	<ul style="list-style-type: none"> • Documenta i dettagli sulla configurazione AWS dell'ambiente in base alla struttura degli account, agli utilizzi dei servizi, ai modelli IAM e ad altre funzionalità principali della configurazione. AWS • Sviluppa diagrammi di architettura delle tue architetture cloud.
Processo	Sviluppa dei playbook di risposta agli incidenti.	<ul style="list-style-type: none"> • Crea un modello per la struttura dei tuoi playbook. • Crea playbook per gli eventi di sicurezza previsti. • Crea playbook per avvisi di sicurezza noti, come i risultati. GuardDuty

Dominio	Elemento di preparazione	Elementi d'azione
Processo	Esegui simulazioni regolari.	<ul style="list-style-type: none"> • Sviluppa una cadenza regolare per eseguire simulazioni di incidenti. • Usa i risultati e le lezioni apprese per mettere a punto il tuo programma di risposta agli incidenti.
Tecnologia	Sviluppa una struttura AWS degli account.	<ul style="list-style-type: none"> • Pianifica una struttura degli account in base alla modalità di separazione dei carichi di lavoro tra AWS account. • Crea un'unità organizzativa di sicurezza con strumenti di sicurezza e un account di archiviazione dei log. • Crea un'unità organizzativa forense con account forensi per ogni regione in cui operi.
Tecnologia	Sviluppa e implementa una strategia di etichettatura che aiuti i rispondenti a identificare la titolarità e il contesto dei risultati.	<ul style="list-style-type: none"> • Pianifica una strategia per l'etichettatura e i tag che desideri associare alle tue risorse. AWS • Implementa e applica la strategia di tagging.

Dominio	Elemento di preparazione	Elementi d'azione
Tecnologia	Aggiorna le informazioni di contatto dell' AWS account.	<ul style="list-style-type: none">• Verifica che negli AWS account siano elencate le informazioni di contatto.• Crea liste di distribuzione e-mail per le informazioni di contatto per rimuovere singoli punti di errore.• Proteggi gli account e-mail associati alle informazioni dell' AWS account.
Tecnologia	Prepara l'accesso agli AWS account.	<ul style="list-style-type: none">• Definisci l'accesso di cui avranno bisogno i soccorritori per rispondere a un incidente.• Implementa, testa e monitora l'accesso.
Tecnologia	Comprendi il panorama delle minacce.	<ul style="list-style-type: none">• Sviluppa modelli di minaccia del tuo ambiente e delle tue applicazioni.• Integra e utilizza l'intelligenza sulle minacce informatiche.

Dominio	Elemento di preparazione	Elementi d'azione
Tecnologia	Seleziona e configura i registri.	<ul style="list-style-type: none"> • Identifica e abilita i registri per le indagini. • Seleziona l'archiviazione dei registri. • Identifica e implementa la conservazione dei log. • Sviluppa un meccanismo per recuperare e interrogare log e artefatti. • Usa i log per avvisare.
Tecnologia	Sviluppa capacità forensi.	<ul style="list-style-type: none"> • Identifica gli artefatti necessari per la raccolta forense. • Acquisisci e proteggi i backup dei sistemi chiave. • Definisci i meccanismi per l'analisi dei log e degli artefatti identificati. • Implementa l'automazione per l'analisi forense.

Si consiglia un approccio iterativo per la preparazione della risposta agli incidenti. Tutti questi elementi di preparazione non possono essere eseguiti dall'oggi al domani; è necessario creare un piano per iniziare in piccolo e migliorare continuamente le capacità di risposta agli incidenti nel tempo.

Operazioni

Le operazioni sono il fulcro dell'esecuzione della risposta agli incidenti. È qui che avvengono le azioni di risposta e riparazione degli incidenti di sicurezza. Le operazioni comprendono le seguenti cinque fasi: rilevamento, analisi, contenimento, rimozione e ripristino. Le descrizioni di queste fasi e degli obiettivi sono disponibili nella Tabella 3.

Tabella 3 — Fasi operative

Fase	Obiettivo
Rilevamento	Identifica un potenziale evento di sicurezza.
Analisi	Determina se un evento di sicurezza è un incidente e valuta la portata dell'incidente.
Contenimento	Riduci al minimo e limita l'ambito dell'evento di sicurezza.
Eradicazione	Rimuovi risorse o artefatti non autorizzati correlati all'evento di sicurezza. Implementa le mitigazioni che hanno causato l'incidente di sicurezza.
Recupero	Ripristina i sistemi a uno stato di sicurezza noto e monitora questi sistemi per verificare che la minaccia non si ripresenti.

Queste fasi dovrebbero servire da guida quando si risponde e si opera sugli incidenti di sicurezza per garantire una risposta efficace e forte. Le azioni effettive che intraprenderai variano a seconda dell'incidente. Un incidente relativo a un ransomware, ad esempio, presenta una serie di passaggi di risposta diversi da quelli di un incidente che coinvolge un bucket Amazon S3 pubblico. Inoltre, questi passaggi non devono essere seguiti necessariamente in sequenza. Dopo il contenimento e la rimozione, potrebbe essere necessario tornare all'analisi per capire se le azioni intraprese sono state efficaci.

Rilevamento

Un avviso è il componente principale della fase di rilevamento. Genera una notifica per avviare il processo di risposta agli incidenti in base all'attività di minaccia dell' AWS account di interesse.

La precisione degli avvisi è difficile; non è sempre possibile determinare con assoluta certezza se un incidente si è verificato, è in corso o se si verificherà in futuro. Ecco alcuni motivi:

- I meccanismi di rilevamento si basano sulla deviazione di base, sugli schemi noti e sulla notifica da parte di entità interne o esterne.

- A causa della natura imprevedibile della tecnologia e delle persone, rispettivamente dei mezzi e degli attori degli incidenti di sicurezza, i valori di base cambiano nel tempo. I modelli anomali emergono attraverso tattiche, tecniche e procedure nuove o modificate per gli attori delle minacce (). TTPs
- Le modifiche alle persone, alla tecnologia e ai processi non vengono incorporate immediatamente nel processo di risposta agli incidenti. Alcune vengono scoperte durante lo svolgimento di un'indagine.

Sorgenti di avviso

È consigliabile prendere in considerazione l'utilizzo delle seguenti fonti per definire gli avvisi:

- Risultati: AWS servizi come [Amazon GuardDuty](#), [Amazon Macie](#) [AWS Security Hub CSPM](#), [Amazon Inspector](#) [AWS Config](#), [IAM Access Analyzer](#) e [Network Access Analyzer](#) generano risultati che possono essere utilizzati per creare avvisi.
- Registri: i log di AWS servizi, infrastrutture e applicazioni archiviati nei bucket e nei gruppi di log di Amazon S3 possono essere analizzati CloudWatch e correlati per generare avvisi.
- Attività di fatturazione: un cambiamento improvviso nell'attività di fatturazione può indicare un evento di sicurezza. Consulta la documentazione sulla [creazione di un allarme di fatturazione per monitorare gli AWS addebiti stimati](#). A tal fine, è necessario tenere sotto controllo questa situazione.
- Intelligence sulle minacce informatiche: se ti abboni a un feed di intelligence sulle minacce informatiche di terze parti, puoi correlare tali informazioni con altri strumenti di registrazione e monitoraggio per identificare potenziali indicatori di eventi.
- Strumenti per i partner: i partner di AWS Partner Network (APN) offrono prodotti di alto livello che possono aiutarti a raggiungere i tuoi obiettivi di sicurezza. Per quanto riguarda la risposta agli incidenti, i prodotti dei partner con endpoint detection and response (EDR) o SIEM possono aiutarti a raggiungere gli obiettivi di risposta agli incidenti. Per ulteriori informazioni, vedere [Security Partner Solutions](#) e [Security Solutions](#) nel Marketplace AWS
- AWS fiducia e sicurezza: Supporto potremmo contattare i clienti se identifichiamo attività abusive o dannose.
- Contatto una tantum: poiché possono essere clienti, sviluppatori o altro personale dell'organizzazione a notare qualcosa di insolito, è importante disporre di un metodo noto e ben pubblicizzato per contattare il team di sicurezza. Le scelte più comuni includono sistemi di biglietteria, indirizzi e-mail di contatto e moduli web. Se la tua organizzazione lavora con il pubblico

in generale, potresti aver bisogno anche di un meccanismo di contatto di sicurezza rivolto al pubblico.

Per ulteriori informazioni sulle funzionalità cloud che puoi utilizzare durante le tue indagini, consulta questo documento [the section called “Appendice A: Definizioni delle funzionalità cloud”](#).

Il rilevamento come parte dell'ingegneria del controllo della sicurezza

I meccanismi di rilevamento sono parte integrante dello sviluppo del controllo della sicurezza. Una volta definiti i controlli direttivi e preventivi, è necessario costruire i relativi controlli investigativi e reattivi. Ad esempio, un'organizzazione stabilisce un controllo direttivo relativo all'utente root di un AWS account, che dovrebbe essere utilizzato solo per attività specifiche e ben definite. Lo associano a un controllo preventivo implementato utilizzando la politica di controllo dei servizi (SCP) di un' AWS organizzazione. Se si verifica un'attività dell'utente root oltre la linea di base prevista, un controllo investigativo implementato con una EventBridge regola e un argomento SNS avviserà il Security Operations Center (SOC). Il controllo reattivo prevede che il SOC selezioni il playbook appropriato, esegua l'analisi e lavori fino alla risoluzione dell'incidente.

Il modo migliore per definire i controlli di sicurezza è la modellazione delle minacce dei carichi di lavoro in esecuzione. AWS La criticità dei controlli investigativi verrà stabilita esaminando l'analisi dell'impatto aziendale (BIA) per il particolare carico di lavoro. Gli avvisi generati dai controlli investigativi non vengono gestiti man mano che arrivano, ma piuttosto in base alla loro criticità iniziale, per essere corretti durante l'analisi. Il set di criticità iniziale aiuta a stabilire le priorità; il contesto in cui si è verificato l'avviso determinerà la sua vera criticità. Ad esempio, un'organizzazione utilizza Amazon GuardDuty come componente del controllo investigativo utilizzato per le istanze EC2 che fanno parte di un carico di lavoro. Il risultato `Impact: EC2/SuspiciousDomainRequest.Reputation` viene generato e ti informa che l'istanza Amazon EC2 elencata all'interno del tuo carico di lavoro sta interrogando un nome di dominio sospettato di essere dannoso. Questo avviso è impostato di default su un livello di gravità basso e, man mano che la fase di analisi procede, è stato stabilito che diverse centinaia di istanze EC2 di questo tipo sono `p4d.24xlarge` state implementate da un attore non autorizzato, con un aumento significativo dei costi operativi dell'organizzazione. A questo punto, il team addetto alla risposta agli incidenti decide di aumentare la criticità di questo avviso, aumentando il senso di urgenza e accelerando ulteriori azioni. Tieni presente che la gravità del GuardDuty rilevamento non può essere modificata.

Implementazioni del controllo investigativo

È importante capire come vengono implementati i controlli investigativi perché aiutano a determinare come verrà utilizzato l'avviso per un particolare evento. Esistono due implementazioni principali dei controlli investigativi tecnici:

- Il rilevamento comportamentale si basa su modelli matematici comunemente denominati apprendimento automatico (ML) o intelligenza artificiale (AI). Il rilevamento viene effettuato per inferenza; pertanto, l'avviso potrebbe non riflettere necessariamente un evento reale.
- Il rilevamento basato su regole è deterministico; i clienti possono impostare i parametri esatti dell'attività su cui ricevere avvisi, e questo è certo.

Le moderne implementazioni di sistemi di rilevamento, come un sistema di rilevamento delle intrusioni (IDS), sono generalmente dotate di entrambi i meccanismi. Di seguito sono riportati alcuni esempi di rilevamenti comportamentali e basati su regole con GuardDuty

- Quando il risultato `Exfiltration:IAMUser/AnomalousBehavior` viene generato, ti informa che «è stata rilevata una richiesta API anomala nel tuo account». Se approfondisci la documentazione, ti viene detto che «Il modello ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari», indicando che questo risultato è di natura comportamentale.
- Per la scoperta `Impact:S3/MaliciousIPCaller`, GuardDuty sta analizzando le chiamate API dal servizio CloudTrail Amazon S3, confrontando `SourceIPAddress` l'elemento di registro con una tabella di indirizzi IP pubblici che include feed di intelligence sulle minacce. Una volta trovata una corrispondenza diretta con una voce, genera il risultato.

Consigliamo di implementare una combinazione di avvisi comportamentali e basati su regole, poiché non è sempre possibile implementare avvisi basati su regole per ogni attività all'interno del modello di minaccia.

Rilevamento basato sulle persone

Fino a questo punto, abbiamo discusso del rilevamento basato sulla tecnologia. L'altra importante fonte di rilevamento proviene da persone interne o esterne all'organizzazione del cliente. Gli addetti ai lavori possono essere definiti come dipendenti o collaboratori, mentre gli estranei sono entità come i ricercatori in materia di sicurezza, le forze dell'ordine, i notiziari e i social media.

Sebbene il rilevamento basato sulla tecnologia possa essere configurato sistematicamente, il rilevamento basato sulle persone si presenta in una varietà di forme come e-mail, biglietti, posta, post di notizie, telefonate e interazioni di persona. Ci si può aspettare che le notifiche di rilevamento basate sulla tecnologia vengano fornite quasi in tempo reale, ma non ci sono aspettative di tempistiche per il rilevamento basato sulle persone. È fondamentale che la cultura della sicurezza incorpori, faciliti e potenzi i meccanismi di rilevamento basati sulle persone per un approccio di difesa approfondito alla sicurezza.

Riepilogo

Per quanto riguarda il rilevamento, è importante disporre di un mix di avvisi basati su regole e basati sul comportamento. Inoltre, è necessario disporre di meccanismi che consentano alle persone, interne ed esterne, di inviare un ticket relativo a un problema di sicurezza. Gli esseri umani possono essere una delle fonti più preziose per gli eventi di sicurezza, quindi è importante disporre di processi che consentano alle persone di esprimere le proprie preoccupazioni. È necessario utilizzare i modelli di minaccia del proprio ambiente per iniziare a rilevare gli edifici. I modelli di minaccia ti aiuteranno a creare avvisi basati sulle minacce più pertinenti al tuo ambiente. Infine, è possibile utilizzare framework come MITRE ATT&CK per comprendere tattiche, tecniche e procedure degli attori delle minacce (). TTPs Il framework MITRE ATT&CK può essere utile da utilizzare come linguaggio comune tra i vari meccanismi di rilevamento.

Analisi

I log, le funzionalità di interrogazione e l'intelligence sulle minacce sono alcuni dei componenti di supporto richiesti dalla fase di analisi. Molti degli stessi log utilizzati per il rilevamento vengono utilizzati anche per l'analisi e richiederanno l'onboarding e la configurazione degli strumenti di interrogazione.

Convalida, analizza e valuta l'impatto degli avvisi

Durante la fase di analisi, viene eseguita un'analisi completa dei registri con l'obiettivo di convalidare gli avvisi, definire l'ambito e valutare l'impatto della possibile compromissione.

- La convalida dell'avviso è il punto di partenza della fase di analisi. I soccorritori cercheranno le voci di registro da varie fonti e interagiranno direttamente con i proprietari del carico di lavoro interessato.
- La fase successiva consiste nell'inventariare tutte le risorse coinvolte e modificare la criticità degli avvisi dopo che le parti interessate concordano sul fatto che è improbabile che si tratti di un falso positivo.

- Infine, l'analisi dell'impatto descrive in dettaglio l'effettiva interruzione dell'attività.

Una volta identificati i componenti del carico di lavoro interessati, è possibile correlare i risultati dell'analisi con l'obiettivo del punto di ripristino (RPO) e l'obiettivo del tempo di ripristino (RTO) del carico di lavoro correlato, adattandoli alla criticità degli avvisi, che avvieranno l'allocazione delle risorse e tutte le attività successive. Non tutti gli incidenti interromperanno direttamente le operazioni di un carico di lavoro che supporta un processo aziendale. Incidenti come la divulgazione di dati sensibili, il furto di proprietà intellettuale o il furto di risorse (come nel caso del mining di criptovalute) potrebbero non interrompere o indebolire immediatamente un processo aziendale, ma possono avere conseguenze in un secondo momento.

Arricchisci i registri e i risultati di sicurezza

Arricchimento con informazioni sulle minacce e contesto organizzativo

Nel corso dell'analisi, gli osservabili di interesse richiedono un arricchimento per una migliore contestualizzazione dell'avviso. Come indicato nella sezione Preparazione, l'integrazione e lo sfruttamento dell'intelligence sulle minacce informatiche possono essere utili per comprendere meglio una scoperta di sicurezza. I servizi di intelligence sulle minacce vengono utilizzati per assegnare la reputazione e attribuire la proprietà a indirizzi IP pubblici, nomi di dominio e hash di file. Questi strumenti sono disponibili come servizi a pagamento e gratuiti.

I clienti che adottano Amazon Athena come strumento di interrogazione dei log ottengono il vantaggio dei job AWS Glue per caricare le informazioni di intelligence sulle minacce sotto forma di tabelle. Le tabelle di threat intelligence possono essere utilizzate nelle query SQL per correlare elementi di log come indirizzi IP e nomi di dominio, fornendo una visione più completa dei dati da analizzare.

AWS non fornisce informazioni sulle minacce direttamente ai clienti, ma servizi come Amazon GuardDuty utilizzano l'intelligence sulle minacce per l'arricchimento e la generazione di risultati. Puoi anche caricare elenchi di minacce personalizzati in GuardDuty base alla tua intelligence sulle minacce.

Arricchimento con l'automazione

L'automazione è parte integrante della Cloud AWS governance. Può essere utilizzata durante le varie fasi del ciclo di vita della risposta agli incidenti.

Per la fase di rilevamento, l'automazione basata su regole inserisce nei log i modelli di interesse del modello di minaccia e intraprende le azioni appropriate, come l'invio di notifiche. La fase di analisi può

sfruttare il meccanismo di rilevamento e inoltrare il corpo di allerta a un motore in grado di interrogare i log e arricchire gli osservabili per la contestualizzazione dell'evento.

Il corpo di allerta, nella sua forma fondamentale, è composto da una risorsa e da un'identità. Ad esempio, è possibile implementare un'automazione CloudTrail per interrogare l'attività dell' AWS API eseguita dall'identità o dalla risorsa dell'organismo di allerta nel momento dell'avviso, fornendo informazioni aggiuntive tra cui `eventSource eventNameSourceIPAddress`, e sull'attività `userAgent` dell'API identificata. Eseguendo queste interrogazioni in modo automatizzato, gli addetti alla risposta possono risparmiare tempo durante il triage e ottenere un contesto aggiuntivo per aiutare a prendere decisioni più informate.

Per un esempio [su come utilizzare l'automazione per arricchire i risultati di AWS Security Hub con i metadati degli account](#), consulta il post del blog [How to enrich Security Hub with Account Metadata](#).

Raccogli e analizza prove forensi

La scienza forense, come menzionato nella [the section called "Preparazione"](#) sezione di questo documento, è il processo di raccolta e analisi degli artefatti durante la risposta agli incidenti. Attivo AWS, è applicabile alle risorse del dominio dell'infrastruttura come l'acquisizione di pacchetti del traffico di rete, il dump della memoria del sistema operativo e alle risorse del dominio di servizio come i log. AWS CloudTrail

Il processo di analisi forense presenta le seguenti caratteristiche fondamentali:

- Coerente: segue i passaggi esatti documentati, senza deviazioni.
- Ripetibile: produce esattamente gli stessi risultati se ripetuto sullo stesso artefatto.
- Conveniente: è documentato pubblicamente e ampiamente adottato.

È importante mantenere una catena di custodia per gli artefatti raccolti durante la risposta agli incidenti. L'utilizzo dell'automazione e la generazione automatica della documentazione di questa raccolta possono essere utili, oltre a memorizzare gli artefatti in archivi di sola lettura. L'analisi deve essere eseguita solo su repliche esatte degli artefatti raccolti per mantenerne l'integrità.

Raccogli gli artefatti pertinenti

Tenendo presenti queste caratteristiche e sulla base degli avvisi pertinenti e della valutazione dell'impatto e della portata, sarà necessario raccogliere i dati che saranno pertinenti per ulteriori indagini e analisi. Vari tipi e fonti di dati che potrebbero essere rilevanti per l'indagine, tra cui log

service/control piani (CloudTrail eventi di dati Amazon S3, log di flusso VPC), dati (metadati e oggetti Amazon S3) e risorse (database, istanze Amazon EC2).

Service/control I log dei piani possono essere raccolti per l'analisi locale o, idealmente, interrogati direttamente utilizzando servizi nativi (ove applicabile). AWS I dati (inclusi i metadati) possono essere interrogati direttamente per ottenere informazioni pertinenti o per acquisire gli oggetti di origine; ad esempio, puoi utilizzare il bucket Amazon S3 e i AWS CLI metadati degli oggetti e acquisire direttamente gli oggetti di origine. Le risorse devono essere raccolte in modo coerente con il tipo di risorsa e il metodo di analisi previsto. Ad esempio, i database possono essere raccolti creando un copy/snapshot sistema che esegue il database, creando uno copy/snapshot dell'intero database stesso o interrogando ed estraendo determinati dati e registri dal database pertinenti all'indagine.

Per le istanze Amazon EC2, è necessario raccogliere un set specifico di dati e eseguire un ordine di raccolta specifico per acquisire e conservare la maggior quantità di dati per analisi e indagini.

In particolare, l'ordine di risposta per acquisire e conservare la maggior quantità di dati da un'istanza Amazon EC2 è il seguente:

1. Acquisizione di metadati dell'istanza: acquisisci i metadati dell'istanza pertinenti all'indagine e alle richieste di dati (ID istanza, tipo, indirizzo IP, VPC/subnet ID, regione, ID Amazon Machine Image (AMI), gruppi di sicurezza collegati, ora di avvio).
2. Abilita le protezioni e i tag delle istanze: abilita le protezioni delle istanze come la protezione dalla terminazione, imposta il comportamento di arresto (se impostato su termina), disabilita gli attributi Delete on Termination per i volumi EBS collegati e applica i tag appropriati sia per la denotazione visiva che per l'uso in possibili automazioni di risposta (ad esempio, dopo aver applicato un tag con nome Status e valore di Quarantine, esegui l'acquisizione forense dei dati e isola l'istanza).
3. Acquisisci disco (istantanee EBS): acquisisci un'istantanea EBS dei volumi EBS collegati. Ogni istantanea contiene le informazioni necessarie per ripristinare i dati (dal momento in cui è stata scattata l'istantanea) su un nuovo volume EBS. Consulta la procedura per eseguire la response/artifact raccolta in tempo reale se utilizzi volumi di Instance Store.
4. Acquisizione di memoria: poiché gli snapshot EBS acquisiscono solo dati che sono stati scritti sul volume Amazon EBS, il che potrebbe escludere i dati archiviati o memorizzati nella cache dalle applicazioni o dal sistema operativo, è imperativo acquisire un'immagine di memoria di sistema utilizzando uno strumento open source o commerciale di terze parti appropriato per acquisire i dati disponibili dal sistema.
5. (Facoltativo) Esegui la risposta in tempo reale/la raccolta di artefatti: esegui la raccolta mirata dei dati (disk/memory/logs) tramite risposta in tempo reale sul sistema solo se il disco o la memoria

non possono essere acquisiti in altro modo o se esiste un motivo aziendale o operativo valido. In questo modo si modificheranno dati e artefatti importanti del sistema.

6. Disattivazione dell'istanza: scollega l'istanza dai gruppi di Auto Scaling, annulla la registrazione dell'istanza dai sistemi di bilanciamento del carico e modifica o applica un profilo di istanza predefinito con autorizzazioni ridotte al minimo o assenti.
7. Isola o contiene l'istanza: verifica che l'istanza sia effettivamente isolata da altri sistemi e risorse all'interno dell'ambiente terminando e impedendo le connessioni attuali e future da e verso l'istanza. Per ulteriori dettagli, consulta la [the section called "Contenimento"](#) sezione di questo documento.
8. Scelta del risponditore: in base alla situazione e agli obiettivi, seleziona una delle seguenti opzioni:
 - Disattivate e spegnete il sistema (scelta consigliata).

Spegnere il sistema una volta acquisite le prove disponibili per verificare la mitigazione più efficace rispetto a possibili impatti futuri sull'ambiente da parte dell'istanza.

- Continua a eseguire l'istanza all'interno di un ambiente isolato dotato di strumentazione per il monitoraggio.

Sebbene non sia consigliato come approccio standard, se una situazione richiede un'osservazione continua dell'istanza (ad esempio quando sono necessari dati o indicatori aggiuntivi per eseguire indagini e analisi complete dell'istanza), potresti prendere in considerazione la chiusura dell'istanza, la creazione di un'AMI dell'istanza e il riavvio dell'istanza nel tuo account forense dedicato all'interno di un ambiente sandbox preattrezzato per essere completamente isolato e configurato con strumentazione per facilitare la quasi continuità monitoraggio dell'istanza (per ad esempio, VPC Flow Logs o VPC Traffic Mirroring).

Note

È essenziale acquisire la memoria prima delle attività di risposta in tempo reale o dell'isolamento o dello spegnimento del sistema per acquisire i dati volatili (e preziosi) disponibili.

Sviluppa narrazioni

Durante l'analisi e le indagini, documenta le azioni intraprese, le analisi eseguite e le informazioni identificate, da utilizzare nelle fasi successive e, infine, in un rapporto finale. Questi resoconti devono essere concisi e precisi e confermare l'inclusione di informazioni pertinenti per verificare l'effettiva

comprensione dell'incidente e mantenere una tempistica accurata. Sono utili anche quando si coinvolgono persone esterne al team principale di risposta agli incidenti. Ecco un esempio:

i Il reparto marketing e vendite ha ricevuto una richiesta di riscatto il 15 marzo 2022 che richiedeva il pagamento in criptovaluta per evitare la pubblicazione pubblica di possibili dati sensibili. Il SOC ha stabilito che il database Amazon RDS appartenente al marketing e alle vendite era accessibile al pubblico il 20 febbraio 2022. Il SOC ha interrogato i log di accesso RDS e ha stabilito che l'indirizzo IP 198.51.100.23 è stato utilizzato il 20 febbraio 2022 con le credenziali appartenenti a Major Mary, uno degli sviluppatori web. mm03434 Il SOC ha interrogato i log di flusso VPC e ha stabilito che circa 256 MB di dati sono stati trasmessi allo stesso indirizzo IP nella stessa data (timestamp 2022-02-20T 15:50 +00Z). Il SOC ha stabilito tramite l'intelligence open source sulle minacce che le credenziali sono attualmente disponibili in testo semplice nell'archivio pubblico. <https://example.com/majormary/rds-utils>

Contenimento

Una definizione di contenimento, in relazione alla risposta agli incidenti, è il processo o l'implementazione di una strategia durante la gestione di un evento di sicurezza che agisce per ridurre al minimo la portata dell'evento di sicurezza e contenere gli effetti dell'uso non autorizzato all'interno dell'ambiente.

Una strategia di contenimento dipende da una miriade di fattori e può variare da un'organizzazione all'altra in termini di applicazione delle tattiche di contenimento, della tempistica e dello scopo. La [Guida alla gestione degli incidenti di sicurezza informatica NIST SP 800-61](#) delinea diversi criteri per determinare la strategia di contenimento appropriata, che include:

- Potenziali danni e furti di risorse
- Necessità di conservare le prove
- Disponibilità del servizio (connettività di rete, servizi forniti a soggetti esterni)
- Tempo e risorse necessari per attuare la strategia
- Efficacia della strategia (contenimento parziale o totale)
- Durata della soluzione (soluzione alternativa di emergenza da rimuovere in quattro ore, soluzione temporanea da rimuovere in due settimane, soluzione permanente)

Per quanto riguarda i servizi AWS attivi, tuttavia, le fasi fondamentali di contenimento possono essere suddivise in tre categorie:

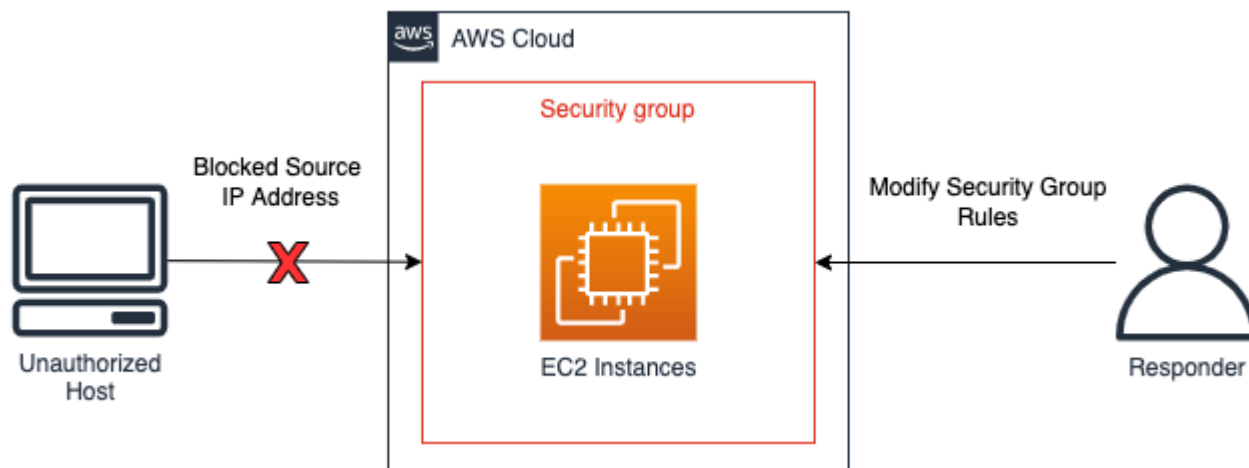
- **Contenimento della fonte:** utilizza il filtraggio e il routing per impedire l'accesso da una determinata fonte.
- **Tecnica e contenimento degli accessi:** rimuovi l'accesso per impedire l'accesso non autorizzato alle risorse interessate.
- **Contenimento della destinazione:** utilizza il filtraggio e il routing per impedire l'accesso a una risorsa di destinazione.

Contenimento della fonte

Il contenimento della fonte è l'uso e l'applicazione del filtraggio o del routing all'interno di un ambiente per impedire l'accesso alle risorse da uno specifico indirizzo IP di origine o intervallo di rete. Di seguito sono evidenziati alcuni esempi di contenimento delle sorgenti tramite AWS servizi:

- **Gruppi di sicurezza:** la creazione e l'applicazione di gruppi di sicurezza di isolamento alle istanze Amazon EC2 o la rimozione di regole da un gruppo di sicurezza esistente può aiutare a contenere il traffico non autorizzato verso un'istanza o una risorsa Amazon EC2. AWS È importante notare che le connessioni tracciate esistenti non verranno interrotte a seguito della modifica dei gruppi di sicurezza: solo il traffico futuro verrà effettivamente bloccato dal nuovo gruppo di sicurezza (consulta [questo Incident Response Playbook](#) e Tracciamento delle connessioni dei gruppi di [sicurezza per ulteriori informazioni sulle connessioni tracciate](#) e non tracciate).
- **Policy:** le policy dei bucket di Amazon S3 possono essere configurate per bloccare o consentire il traffico proveniente da un indirizzo IP, un intervallo di rete o un endpoint VPC. Le policy consentono di bloccare gli indirizzi sospetti e l'accesso al bucket Amazon S3. Ulteriori informazioni sulle policy dei bucket sono disponibili alla pagina [Aggiungere una policy sui bucket utilizzando la console Amazon S3](#).
- **AWS WAF** — Le liste di controllo degli accessi Web (web ACLs) possono essere configurate AWS WAF per fornire un controllo dettagliato sulle richieste Web a cui le risorse rispondono. È possibile aggiungere un indirizzo IP o un intervallo di rete a un set IP configurato su AWS WAF e applicare condizioni di corrispondenza, ad esempio blocco, al set IP. Ciò bloccherà le richieste Web a una risorsa se l'indirizzo IP o gli intervalli di rete del traffico di origine corrispondono a quelli configurati nelle regole del set IP.

Nel diagramma seguente è illustrato un esempio di contenimento dei sorgenti con un analista della risposta agli incidenti che modifica un gruppo di sicurezza di un'istanza Amazon EC2 per limitare le nuove connessioni solo a determinati indirizzi IP. Come indicato nel bullet sui gruppi di sicurezza, le connessioni tracciate esistenti non verranno interrotte a seguito della modifica dei gruppi di sicurezza.



Esempio di contenimento della sorgente

i Note

I gruppi di sicurezza e gli ACL di rete non filtrano il traffico verso Amazon Route 53. Quando contiene un'istanza EC2, se vuoi evitare che entri in contatto con host esterni, assicurati di bloccare esplicitamente anche le comunicazioni DNS.

Tecnica e contenimento degli accessi

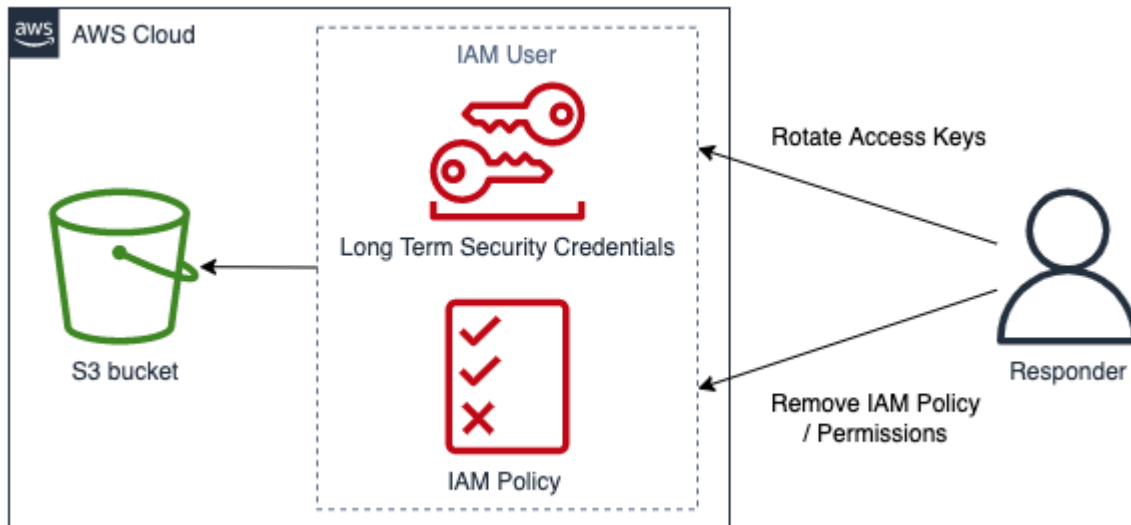
Impedisci l'uso non autorizzato di una risorsa limitando le funzioni e i principali IAM con accesso alla risorsa. Ciò include la limitazione delle autorizzazioni dei responsabili IAM che hanno accesso alla risorsa; include anche la revoca temporanea delle credenziali di sicurezza. Di seguito sono evidenziati esempi di tecniche e contenimento degli accessi tramite i servizi: AWS

- Limita le autorizzazioni: le autorizzazioni assegnate a un principale IAM devono seguire il [principio del privilegio minimo](#). Tuttavia, durante un evento di sicurezza attivo, potrebbe essere necessario limitare ulteriormente l'accesso a una risorsa mirata da parte di uno specifico preside IAM. In questo caso, è possibile contenere l'accesso a una risorsa rimuovendo le autorizzazioni dal principale IAM da contenere. Questa operazione viene eseguita con il servizio IAM e può essere applicata utilizzando Console di gestione AWS, AWS CLI, o un AWS SDK.

- Chiavi di revoca: le chiavi di accesso IAM vengono utilizzate dai dirigenti IAM per accedere o gestire le risorse. [Si tratta di credenziali statiche a lungo termine per firmare le richieste programmatiche all' AWS API AWS CLI or e iniziano con il prefisso AKIA \(per ulteriori informazioni, consulta la sezione Understanding unique ID prefixes negli identificatori IAM\)](#). Per limitare l'accesso a un principale IAM in cui una chiave di accesso IAM è stata compromessa, la chiave di accesso può essere disattivata o eliminata. È importante tenere presente quanto segue:
 - Una chiave di accesso può essere riattivata dopo essere stata disattivata.
 - Una chiave di accesso non è recuperabile una volta eliminata.
 - Un principale IAM può avere fino a due chiavi di accesso alla volta.
 - Gli utenti o le applicazioni che utilizzano la chiave di accesso perderanno l'accesso una volta disattivata o eliminata la chiave.
- Revoca delle credenziali di sicurezza temporanee: [le credenziali di sicurezza temporanee possono essere utilizzate da un'organizzazione per controllare l'accesso alle AWS risorse e iniziano con il prefisso ASIA \(per ulteriori informazioni, consulta la sezione Understanding unique ID prefixes negli identificatori IAM\)](#). Le credenziali temporanee vengono in genere utilizzate dai ruoli IAM e non devono essere ruotate o revocate esplicitamente perché hanno una durata limitata. Nei casi in cui si verifica un evento di sicurezza che coinvolge una credenziale di sicurezza temporanea prima della scadenza della credenziale di sicurezza temporanea, potrebbe essere necessario modificare le autorizzazioni effettive delle credenziali di sicurezza temporanee esistenti. Questa operazione può essere completata [utilizzando](#) il servizio IAM within Console di gestione AWS Le credenziali di sicurezza temporanee possono essere rilasciate anche agli utenti IAM (a differenza dei ruoli IAM); tuttavia, al momento della stesura di questo documento, non è possibile revocare le credenziali di sicurezza temporanee per un utente IAM all'interno di Console di gestione AWS Per gli eventi di sicurezza in cui la chiave di accesso IAM di un utente viene compromessa da un utente non autorizzato che ha creato credenziali di sicurezza temporanee, le credenziali di sicurezza temporanee possono essere revocate utilizzando due metodi:
 - Allega una policy in linea all'utente IAM che impedisca l'accesso in base alla data di emissione del token di sicurezza (per maggiori dettagli, consulta la sezione Negare l'accesso alle credenziali di sicurezza temporanee emesse prima di un orario specifico in [Disabilitazione delle autorizzazioni](#) per le credenziali di sicurezza temporanee).
 - Elimina l'utente IAM che possiede le chiavi di accesso compromesse. Ricrea l'utente se necessario.
- AWS WAF- Alcune tecniche utilizzate da utenti non autorizzati includono schemi di traffico malevoli comuni, come le richieste che contengono SQL injection e cross-site scripting (XSS). AWS WAF

può essere configurato per abbinare e negare il traffico utilizzando queste tecniche utilizzando le istruzioni delle regole integrate. AWS WAF

Un esempio di contenimento della tecnica e degli accessi è riportato nel diagramma seguente, con un operatore che risponde agli incidenti che ruota le chiavi di accesso o rimuove una policy IAM per impedire a un utente IAM di accedere a un bucket Amazon S3.



Esempio di tecnica e contenimento degli accessi

Contenimento della destinazione

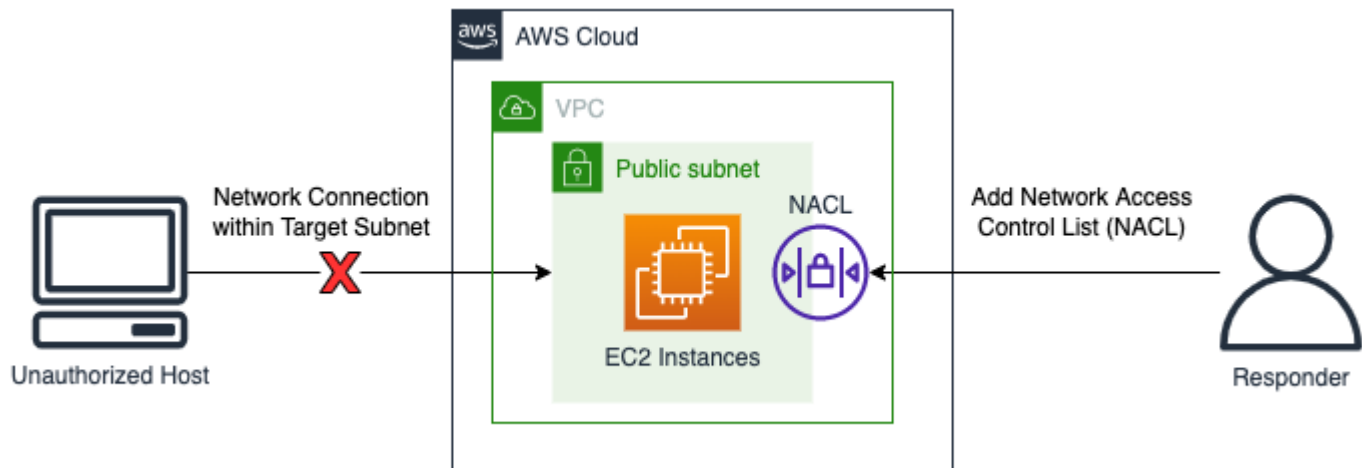
Il contenimento della destinazione è l'applicazione del filtraggio o del routing all'interno di un ambiente per impedire l'accesso a un host o a una risorsa mirati. In alcuni casi, il contenimento della destinazione implica anche una forma di resilienza per verificare che le risorse legittime vengano replicate ai fini della disponibilità; le risorse devono essere separate da queste forme di resilienza per l'isolamento e il contenimento. Alcuni esempi di contenimento della destinazione mediante servizi includono: AWS

- **Rete ACLs** : alle reti ACLs (rete ACLs) configurate su sottoreti che contengono AWS risorse possono essere aggiunte regole di negazione. Queste regole di negazione possono essere applicate per impedire l'accesso a una particolare AWS risorsa; tuttavia, l'applicazione della lista di controllo dell'accesso alla rete (Network ACL) influirà su tutte le risorse della sottorete, non solo sulle risorse a cui si accede senza autorizzazione. Le regole elencate in un ACL di rete vengono elaborate in ordine dall'alto verso il basso, pertanto la prima regola in un ACL di rete esistente deve essere configurata in modo da impedire il traffico non autorizzato verso la risorsa e la sottorete di destinazione. In alternativa, è possibile creare un ACL di rete completamente nuovo con una regola

di negazione singola per il traffico in entrata e in uscita e associato alla sottorete contenente la risorsa di destinazione per impedire l'accesso alla sottorete utilizzando il nuovo ACL di rete.

- Arresto: la chiusura completa di una risorsa può essere efficace nel contenere gli effetti dell'uso non autorizzato. La chiusura di una risorsa impedirà inoltre l'accesso legittimo per esigenze aziendali e impedirà l'ottenimento di dati forensi volatili, quindi questa decisione dovrebbe essere mirata e valutata in base alle politiche di sicurezza dell'organizzazione.
- Isolamento VPCs : i VPC di isolamento possono essere utilizzati per garantire un contenimento efficace delle risorse fornendo al contempo l'accesso al traffico legittimo (ad esempio soluzioni antivirus (AV) o EDR che richiedono l'accesso a Internet o a una console di gestione esterna). I VPC di isolamento possono essere preconfigurati prima di un evento di sicurezza per consentire indirizzi IP e porte validi e le risorse mirate possono essere immediatamente spostate in questo VPC di isolamento durante un evento di sicurezza attivo per contenere la risorsa e consentire al traffico legittimo di essere inviato e ricevuto dalla risorsa interessata durante le fasi successive di risposta all'incidente. Un aspetto importante dell'utilizzo di un VPC di isolamento è che le risorse, come le istanze EC2, devono essere chiuse e riavviate nel nuovo VPC di isolamento prima dell'uso. Le istanze EC2 esistenti non possono essere spostate in un altro VPC o in un'altra zona di disponibilità. A tale scopo, segui i passaggi descritti in [Come posso spostare la mia istanza Amazon EC2 su un'altra sottorete, zona di disponibilità o VPC?](#)
- Gruppi di Auto Scaling e sistemi di bilanciamento del carico: AWS le risorse collegate ai gruppi Auto Scaling e ai sistemi di bilanciamento del carico devono essere scollegate e cancellate come parte delle procedure di contenimento della destinazione. Il distacco e la cancellazione delle risorse possono essere eseguiti utilizzando l'SDK, e. AWS Console di gestione AWS AWS CLI AWS

Un esempio di contenimento della destinazione è illustrato nel diagramma seguente, con un analista della risposta agli incidenti che aggiunge un ACL di rete a una sottorete per bloccare una richiesta di connessione di rete proveniente da un host non autorizzato.



Esempio di contenimento della destinazione

Riepilogo

Il contenimento è una fase del processo di risposta agli incidenti e può essere manuale o automatizzato. La strategia generale di contenimento deve essere in linea con le politiche di sicurezza e le esigenze aziendali di un'organizzazione e verificare che gli effetti negativi siano mitigati nel modo più efficiente possibile prima dell'eradicazione e del ripristino.

Rimozione

Per eradicazione, in relazione alla risposta agli incidenti di sicurezza, si intende la rimozione di risorse sospette o non autorizzate nel tentativo di riportare l'account a uno stato di sicurezza noto. La strategia di eradicazione dipende da molteplici fattori, che dipendono dai requisiti aziendali dell'organizzazione.

La [Guida alla gestione degli incidenti di sicurezza informatica NIST SP 800-61](#) fornisce diversi passaggi per l'eradicazione:

1. Identifica e mitiga tutte le vulnerabilità che sono state sfruttate.
2. Rimuovi malware, materiali inappropriati e altri componenti.
3. Se vengono scoperti altri host interessati (ad esempio, nuove infezioni da malware), ripeti i passaggi di rilevamento e analisi per identificare tutti gli altri host interessati, quindi contenere ed eliminare l'incidente per loro.

Per quanto riguarda AWS le risorse, questo può essere ulteriormente perfezionato attraverso gli eventi rilevati e analizzati tramite i log disponibili o strumenti automatizzati come CloudWatch Logs

e Amazon GuardDuty Tali eventi dovrebbero costituire la base per determinare quali interventi correttivi devono essere eseguiti per ripristinare correttamente l'ambiente a uno stato di sicurezza noto.

La prima fase dell'eliminazione consiste nel determinare quali risorse all'interno dell'account sono state danneggiate. AWS Ciò si ottiene mediante l'analisi delle fonti di dati di registro disponibili, delle risorse e degli strumenti automatizzati.

- Identifica le azioni non autorizzate intraprese dalle identità IAM nel tuo account.
- Identifica accessi o modifiche non autorizzati al tuo account.
- Identifica la creazione di risorse o utenti IAM non autorizzati.
- Identifica i sistemi o le risorse con modifiche non autorizzate.

Una volta identificato l'elenco delle risorse, è necessario valutarle ciascuna per determinare l'impatto aziendale in caso di eliminazione o ripristino della risorsa. Ad esempio, se un server Web ospita la tua applicazione aziendale e la sua eliminazione causerebbe dei tempi di inattività, dovresti prendere in considerazione la possibilità di recuperare la risorsa da backup sicuri verificati o di riavviare il sistema da un'AMI pulita prima di eliminare il server interessato.

Una volta conclusa l'analisi dell'impatto aziendale, utilizzando gli eventi dell'analisi dei log, è necessario accedere agli account ed eseguire le azioni correttive appropriate, ad esempio:

- Ruota o elimina le chiavi: questo passaggio elimina la possibilità dell'attore di continuare a svolgere attività all'interno dell'account.
- Ruota le credenziali utente IAM potenzialmente non autorizzate.
- Elimina risorse non riconosciute o non autorizzate.

Important

Se devi conservare risorse per le tue indagini, valuta la possibilità di effettuare un backup di tali risorse. Ad esempio, se devi conservare un'istanza Amazon EC2 per motivi normativi, di conformità o legali, [crea uno snapshot Amazon EBS](#) prima di rimuovere l'istanza.

- Per le infezioni da malware, potrebbe essere necessario contattare uno AWS Partner o un altro fornitore. AWS non offre strumenti nativi per l'analisi o la rimozione del malware. Tuttavia, se utilizzi il modulo GuardDuty Malware per Amazon EBS, potrebbero essere disponibili consigli per i risultati forniti.

Dopo aver eliminato le risorse interessate identificate, ti AWS consiglia di eseguire una revisione di sicurezza del tuo account. Ciò può essere fatto utilizzando AWS Config regole, utilizzando soluzioni open source come Prowler e/o tramite altri fornitori ScoutSuite. È inoltre consigliabile prendere in considerazione l'esecuzione di scansioni di vulnerabilità sulle risorse pubbliche (Internet) a disposizione per valutare il rischio residuo.

L'eradicazione è una fase del processo di risposta agli incidenti e può essere manuale o automatizzata, a seconda dell'incidente e delle risorse interessate. La strategia generale deve essere in linea con le politiche di sicurezza e le esigenze aziendali dell'organizzazione e verificare che gli effetti negativi siano mitigati dalla rimozione di risorse o configurazioni inappropriate.

Ripristino

Il ripristino è il processo che prevede il ripristino dei sistemi a uno stato sicuro noto, la verifica della sicurezza dei backup o l'assenza dell'impatto dell'incidente prima del ripristino, la verifica del corretto funzionamento dei sistemi dopo il ripristino e la risoluzione delle vulnerabilità associate all'evento di sicurezza.

L'ordine di ripristino dipende dai requisiti dell'organizzazione. Come parte del processo di ripristino, è necessario eseguire un'analisi dell'impatto aziendale per determinare almeno:

- Priorità aziendali o di dipendenza
- Il piano di restauro
- Autenticazione e autorizzazione

La Guida alla gestione degli incidenti di sicurezza informatica NIST SP 800-61 fornisce diversi passaggi per ripristinare i sistemi, tra cui:

- Ripristino dei sistemi da backup puliti.
 - Verificate che i backup vengano valutati prima del ripristino sui sistemi per assicurarvi che l'infezione non sia presente e per prevenire il ripetersi dell'evento di sicurezza.

I backup devono essere valutati regolarmente nell'ambito dei test di disaster recovery per verificare che il meccanismo di backup funzioni correttamente e che l'integrità dei dati soddisfi gli obiettivi dei punti di ripristino.

- Se possibile, utilizzate i backup precedenti al timestamp del primo evento identificato come parte dell'analisi della causa principale.

- Ricostruzione dei sistemi da zero, inclusa la redistribuzione da fonti attendibili utilizzando l'automazione, a volte in un nuovo account. AWS
- Sostituzione di file compromessi con versioni pulite.

È necessario prestare molta attenzione quando si esegue questa operazione. È necessario essere assolutamente certi che il file che si sta recuperando sia noto, sicuro e inalterato dall'incidente.

- Installazione delle patch.
- Modifica delle password.
 - Ciò include le password per i presidi IAM che potrebbero essere state utilizzate in modo improprio.
 - Se possibile, consigliamo di utilizzare i ruoli per i principali e la federazione IAM come parte di una strategia con privilegi minimi.
- Rafforzamento della sicurezza perimetrale della rete (set di regole del firewall, elenchi di controllo degli accessi ai router boundary).

Una volta recuperate le risorse, è importante raccogliere le lezioni apprese per aggiornare le politiche, le procedure e le guide di risposta agli incidenti.

In sintesi, è fondamentale implementare un processo di ripristino che faciliti il ritorno a operazioni sicure note. Il ripristino può richiedere molto tempo e richiede uno stretto collegamento con le strategie di contenimento per bilanciare l'impatto aziendale con il rischio di reinfezione. Le procedure di ripristino devono includere passaggi per il ripristino di risorse e servizi, i principi IAM e l'esecuzione di una revisione della sicurezza dell'account per valutare il rischio residuo.

Conclusioni

Ogni fase operativa ha obiettivi, tecniche, metodologie e strategie uniche. La Tabella 4 riassume queste fasi e alcune delle tecniche e metodologie trattate in questa sezione.

Tabella 4 — Fasi operative: obiettivi, tecniche e metodologie

Fase	Obiettivo	Tecniche e metodologie
Rilevamento	Identifica un potenziale evento di sicurezza.	<ul style="list-style-type: none"> • Controlli di sicurezza per il rilevamento

Fase	Obiettivo	Tecniche e metodologie
		<ul style="list-style-type: none"> • Rilevamento basato sul comportamento e sulle regole • Rilevamento basato sulle persone
Analisi	Determina se l'evento di sicurezza è un incidente e valuta la portata dell'incidente.	<ul style="list-style-type: none"> • Convalida e analizza l'avviso • Log delle query • Informazioni sulle minacce • Automazione
Contenimento	Riduci al minimo e limita l'impatto dell'evento di sicurezza.	<ul style="list-style-type: none"> • Contenimento della fonte • Tecnica e contenimento degli accessi • Contenimento della destinazione
Eradicazione	Rimuovi risorse o artefatti non autorizzati correlati all'evento di sicurezza.	<ul style="list-style-type: none"> • Rotazione o eliminazione delle credenziali compromesse o non autorizzate • Eliminazione non autorizzata di risorse • Rimozione del malware • Scansioni di sicurezza
Recupero	Ripristina i sistemi allo stato corretto noto e monitora questi sistemi per garantire che la minaccia non si ripresenti.	<ul style="list-style-type: none"> • Ripristino del sistema dai backup • Sistemi ricostruiti da zero • File compromessi sostituiti con versioni pulite

Attività post-incidente

Il panorama delle minacce è in continua evoluzione ed è importante essere altrettanto dinamici in termini di capacità dell'organizzazione di proteggere efficacemente gli ambienti. La chiave per il miglioramento continuo è l'iterazione degli esiti degli incidenti e delle simulazioni per migliorare le capacità di rilevare, rispondere e indagare efficacemente su possibili incidenti di sicurezza, riducendo le possibili vulnerabilità, i tempi di risposta e il ripristino di operazioni sicure. I seguenti meccanismi possono aiutarti a verificare che la tua organizzazione sia sempre preparata a rispondere efficacemente grazie alle funzionalità e alle conoscenze più recenti, indipendentemente dalla situazione.

Stabilisci un framework per imparare dagli incidenti

L'implementazione di un framework e di una metodologia tratti dalle lezioni apprese non solo contribuirà a migliorare le capacità di risposta agli incidenti, ma aiuterà anche a prevenire il ripetersi degli incidenti. Imparando da ogni incidente, è possibile evitare di ripetere gli stessi errori, esposizioni o configurazioni errate, non solo migliorando il livello di sicurezza, ma anche riducendo al minimo il tempo perso in situazioni evitabili.

È importante implementare un framework basato sulle lezioni apprese in grado di stabilire e raggiungere, a un livello elevato, i seguenti punti:

- Quando si tiene un framework basato sulle lezioni apprese?
- Cosa comporta il processo basato sulle lezioni apprese?
- Come viene eseguito un framework basato sulle lezioni apprese?
- Chi è coinvolto nel processo e in che modo?
- Come vengono identificate le aree di miglioramento?
- Come farete a garantire che i miglioramenti siano monitorati e implementati in modo efficace?

Oltre a questi risultati di alto livello elencati, è importante assicurarsi di porre le domande giuste per trarre il massimo valore (informazioni che portino a miglioramenti attuabili) dal processo. Considera queste domande per iniziare a promuovere le discussioni sulle lezioni apprese:

- Qual è stato l'incidente?
- Quando è stato identificato per la prima volta l'incidente?
- Come è stato identificato?

- Quali sistemi hanno avvisato dell'attività?
- Quali sistemi, servizi e dati sono stati coinvolti?
- Cosa è successo nello specifico?
- Cosa ha funzionato bene?
- Cosa non ha funzionato bene?
- Quale processo o quali procedure non sono riusciti a scalare per rispondere all'incidente?
- Cosa può essere migliorato nelle seguenti aree:
 - Persone
 - Le persone da contattare erano effettivamente disponibili e l'elenco dei contatti era aggiornato?
 - Le persone presentavano lacune nella formazione o nelle capacità necessarie per rispondere e indagare efficacemente sull'incidente?
 - Le risorse appropriate erano pronte e disponibili?
 - Processo
 - Sono stati seguiti i processi e le procedure?
 - I processi e le procedure erano documentati e disponibili per questo tipo di incidente?
 - Mancavano i processi e le procedure richiesti?
 - Il team di risposta è stato in grado di accedere tempestivamente alle informazioni necessarie per rispondere al problema?
 - Tecnologia
 - I sistemi di avviso esistenti hanno identificato e segnalato efficacemente l'attività?
 - Gli avvisi esistenti devono essere migliorati o è necessario creare nuovi avvisi per questo (tipo di) incidente?
 - Gli strumenti esistenti consentivano un'indagine efficace (ricerca/analisi) dell'incidente?
- Cosa si può fare per identificare prima questo tipo di incidente?
- Cosa si può fare per evitare che questo tipo di incidente si ripeta?
- A chi appartiene il piano di miglioramento e come verifici che sia stato implementato?
- Qual è la tempistica entro cui i monitoring/preventative controlli/processi aggiuntivi devono essere implementati e testati?

Questo elenco non è esaustivo; è destinato a servire come punto di partenza per identificare quali sono le esigenze dell'organizzazione e dell'azienda e come analizzarle per imparare nel modo più

efficace dagli incidenti e migliorare continuamente il livello di sicurezza. La cosa più importante è iniziare incorporando le lezioni apprese come parte standard del processo di risposta agli incidenti, della documentazione e delle aspettative di tutti le parti interessate.

Stabilisci metriche per il successo

Le metriche sono necessarie per misurare, valutare e migliorare in modo efficace le capacità di risposta agli incidenti. Senza metriche, non esiste alcun riferimento rispetto al quale misurare con precisione o addirittura identificare le prestazioni dell'organizzazione (o meno). Esistono alcune metriche comuni alla risposta agli incidenti che rappresentano un buon punto di partenza per un'organizzazione che cerca di stabilire aspettative e riferimenti per lavorare verso l'eccellenza operativa.

Tempo medio di rilevamento

Il tempo medio di rilevamento è il tempo medio necessario per scoprire un possibile incidente di sicurezza. In particolare, si tratta del periodo che intercorre tra il verificarsi del primo indicatore di compromissione e l'identificazione o l'avviso iniziale.

È possibile utilizzare questa metrica per monitorare l'efficacia dei sistemi di rilevamento e allarme. Meccanismi di rilevamento e avviso efficaci sono fondamentali per verificare che eventuali incidenti di sicurezza non persistano all'interno degli ambienti.

Maggiore è il tempo medio di rilevamento, maggiore è la necessità di creare avvisi e meccanismi aggiuntivi o più efficaci per identificare e scoprire possibili incidenti di sicurezza. Più basso è il tempo medio di rilevamento, migliore è il funzionamento dei meccanismi di rilevamento e avviso.

Tempo medio di conferma

Il tempo medio di conferma è il tempo medio necessario per riconoscere e dare priorità a un possibile incidente di sicurezza. In particolare, si tratta del periodo che intercorre tra la generazione di un avviso e il momento in cui un membro del SOC o del personale addetto alla risposta agli incidenti identifica e assegna priorità all'elaborazione dell'avviso.

Puoi utilizzare questa metrica per monitorare l'efficienza con cui il tuo team elabora e assegna priorità agli avvisi. Se il team non è in grado di identificare e dare priorità agli avvisi in modo efficace, le risposte saranno ritardate e inefficaci.

Maggiore è il tempo medio di risposta, maggiore è la necessità di verificare che il team disponga delle risorse e della formazione adeguate per riconoscere e dare priorità rapidamente a un possibile

incidente di sicurezza ai fini della risposta. Più basso è il tempo medio per il riscontro, più il team risponde meglio agli avvisi di sicurezza, dimostrando di essere preparato in modo efficace e in grado di stabilire correttamente le priorità.

Tempo medio di risposta

Il tempo medio di risposta è il tempo medio necessario per iniziare la risposta iniziale a un possibile incidente di sicurezza. In particolare, si tratta del periodo che intercorre tra l'avviso iniziale o la scoperta di un possibile incidente di sicurezza e le prime azioni intraprese per rispondere. È simile al tempo medio di conferma, ma corrisponde alla misurazione di specifiche azioni di risposta (ad esempio, acquisizione di dati di sistema, contenimento del sistema) rispetto al semplice riconoscimento o riconoscimento della situazione.

Puoi utilizzare questa metrica per monitorare la tua preparazione a rispondere agli incidenti di sicurezza. Come accennato, la preparazione è fondamentale per una risposta efficace. Fate riferimento alla [the section called "Preparazione"](#) sezione di questo documento.

Maggiore è il tempo medio di risposta, maggiore è la necessità di verificare che il team sia adeguatamente formato su come rispondere, in modo che i processi di risposta siano documentati e utilizzati in modo efficace. Più basso è il tempo medio di risposta, più il team è in grado di identificare una risposta appropriata agli avvisi identificati ed eseguire le azioni di risposta necessarie per iniziare il percorso verso operazioni sicure.

Tempo medio di contenimento

Il tempo medio di contenimento è il tempo medio necessario per contenere un possibile incidente di sicurezza. In particolare, si tratta del periodo che intercorre tra l'avviso iniziale o la scoperta di un possibile incidente di sicurezza e il completamento delle azioni di risposta che impediscono efficacemente all'aggressore o ai sistemi compromessi di arrecare ulteriori danni.

Puoi utilizzare questa metrica per monitorare la capacità del tuo team di mitigare o contenere possibili incidenti di sicurezza. L'incapacità di contenere in modo rapido ed efficace i possibili incidenti di sicurezza aumenta l'impatto, la portata e l'esposizione a possibili ulteriori compromessi.

Maggiore è il tempo medio di contenimento, maggiore è la necessità di sviluppare conoscenze e capacità per mitigare e contenere in modo rapido ed efficace gli incidenti di sicurezza che si verificano. Più basso è il tempo medio di contenimento, più il team è in grado di comprendere e utilizzare le misure necessarie per mitigare e contenere le minacce identificate, al fine di ridurre l'impatto, la portata e il rischio per l'azienda.

Tempo medio di ripristino

Il tempo medio di ripristino è il tempo medio necessario per ripristinare completamente le operazioni in sicurezza da un possibile incidente di sicurezza. In particolare, si tratta del periodo che intercorre tra l'avviso iniziale o la scoperta di un possibile incidente di sicurezza e il momento in cui l'azienda torna a operare normalmente e in sicurezza senza risentire dell'incidente.

Puoi utilizzare questa metrica per monitorare l'efficacia dei tuoi team nel riportare sistemi, account e ambienti a operazioni sicure dopo un incidente di sicurezza. L'incapacità di ripristinare le operazioni sicure in modo rapido o efficace non solo può avere un impatto sulla sicurezza, ma può anche aumentare l'impatto e i costi per l'azienda e le sue operazioni.

Maggiore è il tempo medio di ripristino, maggiore è la necessità di preparare i team e gli ambienti a disporre dei meccanismi appropriati (ad esempio, processi di failover e CI/CD pipeline per ridistribuire in sicurezza sistemi puliti) per ridurre al minimo l'impatto degli incidenti di sicurezza sulle operazioni e sull'azienda. Più basso è il tempo medio di ripristino, più i team sono efficaci nel ridurre al minimo l'impatto degli incidenti di sicurezza sulle operazioni e sull'azienda.

Tempo di permanenza dell'aggressore

Il tempo di permanenza dell'attaccante è il tempo medio in cui un utente non autorizzato ha accesso a un sistema o a un ambiente. È simile al tempo medio di contenimento, tranne per il fatto che l'intervallo di tempo inizia con l'ora iniziale in cui l'aggressore ha ottenuto l'accesso al sistema o agli ambienti, che potrebbe essere precedente all'avviso o alla scoperta iniziale.

È possibile utilizzare questa metrica per tenere traccia del grado di interazione di molti sistemi e meccanismi per ridurre la quantità di tempo, accesso e opportunità che un aggressore o una minaccia hanno di influire sull'ambiente. Ridurre il tempo di permanenza degli aggressori dovrebbe essere una priorità assoluta per i team e l'azienda.

Maggiore è il tempo di permanenza degli aggressori, maggiore è la necessità di identificare quali parti del processo di risposta agli incidenti devono essere migliorate per garantire che i team siano in grado di ridurre al minimo l'impatto e la portata delle minacce o degli attacchi nei vostri ambienti. Minore è il tempo di permanenza degli aggressori, più i team sono in grado di ridurre al minimo il tempo e le opportunità che una minaccia o un aggressore hanno a disposizione all'interno degli ambienti, riducendo in ultima analisi il rischio e l'impatto sulle operazioni e sull'azienda.

Riepilogo delle metriche

La definizione e il monitoraggio delle metriche per la risposta agli incidenti consente di misurare, valutare e migliorare in modo efficace le capacità di risposta agli incidenti. A tal fine, in questa

sezione sono state evidenziate diverse metriche comuni di risposta agli incidenti. La Tabella 5 riassume queste metriche.

Tabella 5 — Metriche di risposta agli incidenti

Metrica	Description
Tempo medio di rilevamento	Tempo medio necessario per scoprire un possibile incidente di sicurezza
Tempo medio di conferma	Tempo medio necessario per riconoscere (e dare priorità) a un possibile incidente di sicurezza
Tempo medio di risposta	Tempo medio necessario per avviare la risposta iniziale a un possibile incidente di sicurezza
Tempo medio di contenimento	Tempo medio necessario per contenere un possibile incidente di sicurezza
Tempo medio di ripristino	Tempo medio necessario per ripristinare completamente le operazioni in modo sicuro da un possibile incidente di sicurezza
Tempo di permanenza dell'attaccante	Tempo medio di accesso a un sistema o a un ambiente da parte di un utente malintenzionato

Utilizza indicatori di compromesso () IOCs

Un indicatore di compromissione (IOC) è un artefatto osservato in o su una rete, sistema o ambiente in grado (con un elevato livello di sicurezza) di identificare attività dannose o incidenti di sicurezza. IOCs possono esistere in una varietà di forme, tra cui indirizzi IP, domini, artefatti a livello di rete come flag o payload TCP, artefatti a livello di sistema o host come eseguibili, nomi di file e hash, voci di file di registro o voci di registro e altro ancora. Possono anche essere una combinazione di elementi o attività, come l'esistenza di elementi o artefatti specifici su un sistema (un determinato file o set di file ed elementi del registro), azioni eseguite in un determinato ordine (accesso a un sistema da un determinato IP seguito da comandi anomali specifici) o attività di rete (traffico anomalo in

entrata o in uscita da determinati domini) che possono indicare una minaccia, un attacco o un metodo di attacco specifico ologia.

Mentre lavori per migliorare in modo iterativo il tuo programma di risposta agli incidenti, dovresti implementare un framework da raccogliere, gestire e utilizzare IOCs come meccanismo per creare e migliorare continuamente i rilevamenti e gli avvisi e migliorare la velocità e l'efficacia delle indagini. È possibile iniziare incorporando la raccolta e la gestione di IOCs nelle fasi di analisi e indagine dei processi di risposta agli incidenti. Identificando, raccogliendo e archiviando in modo proattivo IOCs come parte standard del processo, è possibile creare un archivio di dati (come parte di un programma di intelligence sulle minacce più completo) che a sua volta può essere utilizzato per migliorare i rilevamenti e gli avvisi esistenti, creare rilevamenti e avvisi aggiuntivi, identificare dove e quando un artefatto è stato rilevato in precedenza, creare e fare riferimento alla documentazione su come venivano eseguite le indagini in precedenza IOCs, coinvolgendo la corrispondenza e altro ancora.

Istruzione e formazione continue

L'istruzione e la formazione sono sforzi continui e in continua evoluzione che devono essere perseguiti e mantenuti in modo mirato. Esistono diversi meccanismi per verificare che il team mantenga la consapevolezza, le conoscenze e le capacità adeguate all'evoluzione dello stato della tecnologia e al panorama delle minacce.

Un meccanismo consiste nell'utilizzare la formazione continua come parte standard degli obiettivi e delle operazioni dei team. Come indicato nella sezione Preparazione, il personale addetto alla risposta agli incidenti e le parti interessate devono essere formati in modo efficace su come rilevare, rispondere e indagare sugli incidenti interni. AWS Tuttavia, l'istruzione non è uno sforzo fatto a mano. La formazione deve essere continuamente perseguita per verificare che il team mantenga la conoscenza degli ultimi progressi tecnologici, degli aggiornamenti e dei miglioramenti che possono essere sfruttati per migliorare l'efficacia e l'efficienza della risposta, nonché delle aggiunte o degli aggiornamenti ai dati che possono essere sfruttati per migliorare l'indagine e l'analisi.

Un altro meccanismo consiste nel verificare che le simulazioni vengano eseguite regolarmente (ad esempio trimestralmente) e incentrate su risultati specifici per l'azienda. Fate riferimento alla [the section called “Esegui simulazioni regolari”](#) sezione di questo documento.

Sebbene l'esecuzione di esercizi iniziali da tavolo sia un ottimo modo per generare una base iniziale di miglioramento, i test continui sono fondamentali per ottenere miglioramenti duraturi e mantenere una rappresentazione up-to-date accurata dello stato attuale delle operazioni. Effettuando test sulla base delle situazioni di sicurezza più recenti e critiche e delle funzionalità di risposta più importanti o più recenti e incorporando le lezioni apprese nel corso dell'istruzione e delle operazioni, processes/

procedures verificheranno che siete in grado di migliorare continuamente i processi di risposta e il programma nel suo complesso.

Conclusioni

Mentre proseguite il vostro percorso verso il cloud, è importante prendere in considerazione i concetti fondamentali di risposta agli incidenti di sicurezza per il vostro AWS ambiente. Puoi combinare i controlli disponibili, le funzionalità cloud e le opzioni di riparazione per aiutarti a migliorare la sicurezza del tuo ambiente cloud. Puoi anche iniziare in piccolo e poi iterare adottando funzionalità di automazione che migliorano la velocità di risposta, in modo da essere meglio preparato quando si verificano eventi di sicurezza.

Collaboratori

I collaboratori attuali e passati a questo documento includono:

- Anna McAbee, architetto senior di soluzioni di sicurezza, Amazon Web Services
- Freddy Kasprzykowski, consulente senior per la sicurezza, Amazon Web Services
- Jason Hurst, ingegnere senior della sicurezza, Amazon Web Services
- Jonathon Poling, consulente principale per la sicurezza, Amazon Web Services
- Josh Du Lac, Senior Manager, Architettura delle soluzioni di sicurezza, Amazon Web Services
- Paco Hope, ingegnere principale della sicurezza, Amazon Web Services
- Ryan Tick, ingegnere senior della sicurezza, Amazon Web Services
- Steve de Vera, ingegnere senior della sicurezza, Amazon Web Services

Appendice A: Definizioni delle funzionalità cloud

AWS offre oltre 200 servizi cloud e migliaia di funzionalità. Molti di questi offrono funzionalità native di investigazione, prevenzione e risposta, mentre altri possono essere utilizzati per progettare soluzioni di sicurezza personalizzate. Questa sezione include un sottoinsieme dei servizi più rilevanti per la risposta agli incidenti nel cloud.

Argomenti

- [Registrazione ed eventi](#)
- [Visibilità e avvisi](#)
- [Automazione di](#)

- [Archiviazione sicura](#)
- [Funzionalità di sicurezza future e personalizzate](#)

Registrazione ed eventi

[AWS CloudTrail](#)— AWS CloudTrail servizio che consente la governance, la conformità, il controllo operativo e il controllo dei rischi dei conti. AWS Con CloudTrail, puoi registrare, monitorare continuamente e conservare le attività dell'account relative alle azioni tra AWS i servizi. CloudTrail fornisce la cronologia degli eventi relativi all'attività dell' AWS account, incluse le azioni intraprese tramite gli strumenti a riga di comando e altri AWS servizi. Console di gestione AWS AWS SDKs Questa cronologia degli eventi semplifica l'analisi della sicurezza, il monitoraggio delle modifiche alle risorse e la risoluzione dei problemi. CloudTrail registra due diversi tipi di azioni AWS API:

- CloudTrail gli eventi di gestione (noti anche come operazioni del piano di controllo) mostrano le operazioni di gestione eseguite sulle risorse AWS dell'account. Ciò include azioni come la creazione di un bucket Amazon S3 e l'impostazione della registrazione.
- CloudTrail gli eventi relativi ai dati (noti anche come operazioni sul piano dati) mostrano le operazioni sulle risorse eseguite su o all'interno di una risorsa del tuo account. AWS Queste operazioni sono spesso attività ad alto volume. Ciò include azioni come l'attività dell'API a livello di oggetto di Amazon S3 (ad esempio `GetObjectDeleteObject`, e le operazioni `PutObject` API) e l'attività di invocazione della funzione Lambda.

[AWS Config](#)— AWS Config è un servizio che consente ai clienti di valutare, controllare e valutare le configurazioni delle risorse. AWS AWS Config monitora e registra continuamente le configurazioni AWS delle risorse e consente di automatizzare la valutazione delle configurazioni registrate rispetto alle configurazioni desiderate. Con AWS Config, i clienti possono esaminare le modifiche nelle configurazioni e nelle relazioni tra le AWS risorse, manualmente o automaticamente, la cronologia dettagliata delle configurazioni delle risorse e determinare la conformità complessiva rispetto alle configurazioni specificate nelle linee guida del cliente. Ciò consente di semplificare il controllo della conformità, l'analisi della sicurezza, la gestione delle modifiche e la risoluzione dei problemi operativi.

[Amazon EventBridge](#) — Amazon EventBridge offre un flusso quasi in tempo reale di eventi di sistema che descrivono i cambiamenti nelle AWS risorse o quando le chiamate API vengono pubblicate da AWS CloudTrail. Utilizzando semplici regole che puoi configurare rapidamente, puoi abbinare gli eventi e indirizzarli a una o più funzioni o flussi di destinazione. EventBridge viene a conoscenza dei cambiamenti operativi man mano che si verificano. EventBridge può rispondere a questi cambiamenti operativi e adottare le misure correttive necessarie, inviando messaggi per rispondere all'ambiente,

attivando funzioni, apportando modifiche e acquisendo informazioni sullo stato. Alcuni servizi di sicurezza, come Amazon GuardDuty, producono i loro risultati sotto forma di EventBridge eventi. Molti servizi di sicurezza offrono anche la possibilità di inviare i propri output ad Amazon S3.

Log di accesso di Amazon S3: se le informazioni sensibili sono archiviate in un bucket Amazon S3, i clienti possono abilitare i log di accesso di Amazon S3 per registrare ogni caricamento, download e modifica di tali dati. Questo registro è separato e si aggiunge ai CloudTrail log che registrano le modifiche al bucket stesso (come la modifica delle politiche di accesso e delle politiche del ciclo di vita). Vale la pena notare che i record dei log di accesso vengono forniti con la massima diligenza possibile. La maggior parte delle richieste di un bucket correttamente configurato per la registrazione determinano la consegna di un report del log. La completezza e la tempestività della registrazione del server non è tuttavia garantita.

[Amazon CloudWatch Logs](#): i clienti possono utilizzare Amazon CloudWatch Logs per monitorare, archiviare e accedere ai file di registro provenienti da sistemi operativi, applicazioni e altre fonti in esecuzione su istanze Amazon EC2 con un agente Logs. CloudWatch CloudWatch I log possono essere una destinazione per le query DNS di Route 53 AWS CloudTrail, i log di flusso VPC, le funzioni Lambda e altro. I clienti possono quindi recuperare i dati di registro associati da Logs. CloudWatch

[Amazon VPC Flow Logs](#): VPC Flow Logs consente ai clienti di acquisire informazioni sul traffico IP in entrata e in uscita dalle interfacce di rete in VPC. Dopo aver abilitato i log di flusso, possono essere trasmessi in streaming ad Amazon CloudWatch Logs e Amazon S3. VPC Flow Logs aiuta i clienti con una serie di attività come la risoluzione dei motivi per cui il traffico specifico non raggiunge un'istanza, la diagnosi delle regole dei gruppi di sicurezza eccessivamente restrittive e l'utilizzo come strumento di sicurezza per monitorare il traffico verso le istanze EC2. Utilizza la versione più recente della registrazione del flusso VPC per ottenere i campi più affidabili.

[AWS WAF Registri](#): AWS WAF supporta la registrazione completa di tutte le richieste Web esaminate dal servizio. I clienti possono archivarli in Amazon S3 per soddisfare i requisiti di conformità e controllo, nonché per il debug e l'analisi forense. Questi registri aiutano i clienti a determinare la causa principale delle regole avviate e delle richieste web bloccate. I log possono essere integrati con strumenti SIEM e di analisi dei log di terze parti.

Log delle [query di Route 53 Resolver: i log](#) delle query di Route 53 Resolver consentono di registrare tutte le query DNS effettuate dalle risorse all'interno di Amazon Virtual Private Cloud (Amazon VPC). Che si tratti di un'istanza Amazon EC2, di una AWS Lambda funzione o di un contenitore, se risiede nel tuo Amazon VPC ed effettua una query DNS, questa funzionalità la registrerà; potrai quindi esplorare e comprendere meglio come funzionano le tue applicazioni.

Altri AWS log: rilascia AWS continuamente caratteristiche e funzionalità del servizio per i clienti con nuove funzionalità di registrazione e monitoraggio. Per informazioni sulle funzionalità disponibili per ogni AWS servizio, consulta la nostra documentazione pubblica.

Visibilità e avvisi

[AWS Security Incident Response](#)— AWS Security Incident Response è un servizio completo che aiuta le organizzazioni a gestire gli eventi di sicurezza durante tutto il loro ciclo di vita combinando funzionalità automatizzate con il supporto umano esperto. Il servizio sfrutta funzionalità automatizzate di monitoraggio e indagine per liberare risorse organizzative mantenendo al contempo una supervisione vigile della sicurezza e, quando si verificano eventi di sicurezza, facilita la comunicazione e il coordinamento accelerati tra le parti interessate per tempi di risposta rapidi. Il servizio supporta diversi casi d'uso, tra cui la preparazione e la simulazione di eventi di sicurezza, la risposta agli incidenti attivi e la reportistica e l'analisi post-incidente semplificate, garantendo che le organizzazioni siano ben attrezzate per gestire le sfide di sicurezza in ogni fase.

[AWS Security Hub CSPM](#)— AWS Security Hub CSPM offre ai clienti una visione completa degli avvisi di sicurezza ad alta priorità e degli stati di conformità tra gli account. AWS Security Hub CSPM aggrega, organizza e dà priorità alle rilevazioni delle minacce provenienti da servizi AWS come Amazon, Amazon Inspector, GuardDuty Amazon Macie e soluzioni. AWS Partner I risultati sono riassunti visivamente su dashboard integrate con grafici e tabelle utilizzabili. È inoltre possibile monitorare continuamente l'ambiente utilizzando controlli di conformità automatizzati basati sulle AWS migliori pratiche e sugli standard di settore seguiti dall'organizzazione.

[Amazon GuardDuty](#) — Amazon GuardDuty è un servizio gestito di rilevamento delle minacce che monitora continuamente comportamenti dannosi o non autorizzati per aiutare i clienti a proteggere AWS account e carichi di lavoro. Monitora attività come chiamate API insolite o implementazioni potenzialmente non autorizzate, indicando possibili compromissioni dell'account o delle risorse delle istanze Amazon EC2, dei bucket Amazon S3 o la ricognizione da parte di malintenzionati.

GuardDuty identifica i sospetti malintenzionati tramite feed integrati di intelligence sulle minacce che utilizzano l'apprendimento automatico per rilevare anomalie nell'attività dell'account e del carico di lavoro. Quando viene rilevata una potenziale minaccia, il servizio invia un avviso di sicurezza dettagliato alla console e agli eventi. GuardDuty CloudWatch Ciò rende gli avvisi utilizzabili e semplici da integrare nei sistemi di gestione degli eventi e del flusso di lavoro esistenti.

GuardDuty offre anche due componenti aggiuntivi per monitorare le minacce con servizi specifici: Amazon GuardDuty per la protezione di Amazon S3 e Amazon GuardDuty per la protezione Amazon EKS. La protezione di Amazon S3 consente di monitorare GuardDuty le operazioni API a livello di

oggetto per identificare potenziali rischi di sicurezza per i dati all'interno dei bucket Amazon S3. La protezione Kubernetes consente di GuardDuty rilevare attività sospette e potenziali compromissioni dei cluster Kubernetes all'interno di Amazon EKS.

[Amazon Macie — Amazon Macie](#) è un servizio di sicurezza basato sull'intelligenza artificiale che aiuta a prevenire la perdita di dati rilevando, classificando e proteggendo automaticamente i dati sensibili archiviati in. AWS Macie utilizza l'apprendimento automatico (ML) per riconoscere dati sensibili come le informazioni di identificazione personale (PII) o la proprietà intellettuale, assegnare un valore aziendale e fornire visibilità su dove vengono archiviati questi dati e su come vengono utilizzati nell'organizzazione. Amazon Macie monitora continuamente l'attività di accesso ai dati per rilevare eventuali anomalie e invia avvisi quando rileva un rischio di accesso non autorizzato o fughe involontarie di dati.

[Regole di AWS Config](#)— Una AWS Config regola rappresenta le configurazioni preferite per una risorsa e viene valutata in base alle modifiche di configurazione sulle risorse pertinenti, come registrato da. AWS Config È possibile visualizzare i risultati della valutazione di una regola rispetto alla configurazione di una risorsa su una dashboard. Utilizzando AWS Config le regole, è possibile valutare la conformità generale e lo stato di rischio dal punto di vista della configurazione, visualizzare le tendenze di conformità nel tempo e scoprire quale modifica della configurazione ha causato la mancata conformità di una risorsa a una regola.

[AWS Trusted Advisor](#)— AWS Trusted Advisor è una risorsa online che consente di ridurre i costi, aumentare le prestazioni e migliorare la sicurezza ottimizzando l' AWS ambiente. Trusted Advisor fornisce indicazioni in tempo reale per aiutarvi a fornire le vostre risorse seguendo le AWS migliori pratiche. La serie completa di Trusted Advisor controlli, inclusa l'integrazione CloudWatch degli eventi, è disponibile per i clienti del piano Business ed Enterprise Support.

[Amazon CloudWatch](#): Amazon CloudWatch è un servizio di monitoraggio delle Cloud AWS risorse e delle applicazioni su cui esegui AWS. Puoi utilizzarlo CloudWatch per raccogliere e tracciare metriche, raccogliere e monitorare file di registro, impostare allarmi e reagire automaticamente ai cambiamenti nelle tue AWS risorse. CloudWatch può monitorare AWS risorse, come istanze Amazon EC2, tabelle Amazon DynamoDB e istanze Amazon RDS DB, nonché i parametri personalizzati generati dalle tue applicazioni e servizi e tutti i file di log generati dalle tue applicazioni. Puoi usare Amazon CloudWatch per ottenere visibilità a livello di sistema sull'utilizzo delle risorse, sulle prestazioni delle applicazioni e sullo stato operativo. Puoi utilizzare queste informazioni per reagire di conseguenza e mantenere l'applicazione funzionante senza intoppi.

[Amazon Inspector](#) — Amazon Inspector è un servizio di valutazione della sicurezza automatizzato che aiuta a migliorare la sicurezza e la conformità delle applicazioni distribuite su. AWS Amazon

Inspector valuta automaticamente le applicazioni per rilevare vulnerabilità o deviazioni dalle best practice. Dopo aver eseguito una valutazione, Amazon Inspector produce un elenco dettagliato di risultati di sicurezza con priorità in base al livello di gravità. Questi risultati possono essere esaminati direttamente o come parte di report di valutazione dettagliati disponibili tramite la console o l'API di Amazon Inspector.

[Amazon Detective](#) — Amazon Detective è un servizio di sicurezza che raccoglie automaticamente i dati di log dalle tue AWS risorse e utilizza l'apprendimento automatico, l'analisi statistica e la teoria dei grafi per creare un set di dati collegato che ti consente di condurre indagini di sicurezza più rapide ed efficienti. Detective può analizzare trilioni di eventi da più fonti di dati come VPC Flow Logs e GuardDuty creare automaticamente una visualizzazione unificata e interattiva delle tue risorse, degli utenti e delle interazioni tra loro nel tempo. CloudTrail Con questa visualizzazione unificata, puoi visualizzare tutti i dettagli e il contesto in un unico posto per identificare le ragioni alla base dei risultati, approfondire le attività storiche pertinenti e determinare rapidamente la causa principale.

Automazione di

[AWS Lambda](#) — AWS Lambda è un servizio di elaborazione serverless che esegue il codice in risposta agli eventi e gestisce automaticamente le risorse di elaborazione sottostanti per te. Puoi usare Lambda per estendere altri AWS servizi con logica personalizzata o creare servizi di backend personalizzati che operano su AWS scala, prestazioni e sicurezza. Lambda esegue il codice su un'infrastruttura di calcolo ad alta disponibilità ed esegue l'amministrazione delle risorse di calcolo per te. Ciò include la manutenzione di server e sistemi operativi, il provisioning della capacità e la scalabilità automatica, l'implementazione di codice e patch di sicurezza e il monitoraggio e la registrazione del codice. Tutto quello che devi fare è fornire il codice.

[AWS Step Functions](#) — AWS Step Functions semplifica il coordinamento dei componenti delle applicazioni e dei microservizi distribuiti utilizzando flussi di lavoro visivi. Step Functions fornisce una console grafica per organizzare e visualizzare i componenti dell'applicazione in una serie di passaggi. Ciò semplifica la creazione e l'esecuzione di applicazioni a più fasi. Step Functions avvia e tiene traccia automaticamente di ogni passaggio e riprova in caso di errori, in modo che l'applicazione venga eseguita nell'ordine e come previsto.

Step Functions registra lo stato di ogni passaggio, così quando qualcosa va storto, puoi diagnosticare ed eseguire rapidamente il debug dei problemi. Puoi modificare e aggiungere passaggi senza scrivere codice, in modo da far evolvere la tua applicazione e innovare più velocemente. AWS Step Functions fa parte di AWS Serverless e semplifica l'orchestrazione delle funzioni per le applicazioni AWS Lambda serverless. Puoi anche utilizzare Step Functions per l'orchestrazione dei microservizi utilizzando risorse di calcolo come Amazon EC2 e Amazon ECS.

[AWS Systems Manager](#): AWS Systems Manager offre visibilità e controllo dell'infrastruttura su AWS. Systems Manager fornisce un'interfaccia utente unificata che consente di visualizzare i dati operativi da più AWS servizi e consente di automatizzare le attività operative tra le AWS risorse. Con Systems Manager, puoi raggruppare le risorse per applicazione, visualizzare i dati operativi per il monitoraggio e la risoluzione dei problemi e agire sui tuoi gruppi di risorse. Systems Manager può mantenere le istanze nello stato definito, eseguire modifiche su richiesta, come l'aggiornamento delle applicazioni o l'esecuzione di script di shell, ed eseguire altre attività di automazione e applicazione di patch.

Archiviazione sicura

[Amazon Simple Storage Service](#): Amazon S3 è uno storage di oggetti progettato per archiviare e recuperare qualsiasi quantità di dati da qualsiasi luogo. È progettato per offrire una durabilità del 99,99999% e archivia i dati per milioni di applicazioni utilizzate dai leader di mercato in ogni settore. Amazon S3 offre una sicurezza completa ed è progettato per aiutarti a soddisfare i requisiti normativi. Offre ai clienti flessibilità nei metodi utilizzati per gestire i dati per l'ottimizzazione dei costi, il controllo degli accessi e la conformità. Amazon S3 offre query-in-place funzionalità che consentono di eseguire potenti analisi direttamente sui dati archiviati in Amazon S3. Amazon S3 è un servizio di cloud storage altamente supportato, con integrazione da una delle più grandi community di soluzioni di terze parti, partner integratori di sistemi e altri servizi. AWS

[Amazon Glacier — Amazon](#) Glacier è un servizio di cloud storage sicuro, durevole ed estremamente economico per l'archiviazione dei dati e il backup a lungo termine. È progettato per offrire una durabilità del 99,339%, offre una sicurezza completa ed è progettato per aiutarti a soddisfare i requisiti normativi. Amazon Glacier query-in-place offre funzionalità che ti consentono di eseguire potenti analisi direttamente sui dati di archivio inattivi. Per mantenere i costi bassi ma adatti a diverse esigenze di recupero, Amazon Glacier offre tre opzioni per l'accesso agli archivi, da pochi minuti a diverse ore.

Funzionalità di sicurezza future e personalizzate

I servizi e le funzionalità sopra menzionati non sono un elenco esaustivo. AWS aggiunge continuamente nuove funzionalità. Per ulteriori informazioni, ti invitiamo a consultare le pagine [What's New at AWS](#) e [AWS Cloud Security](#). Oltre ai servizi di sicurezza AWS offerti come servizi cloud nativi, potresti essere interessato a sviluppare le tue capacità oltre AWS ai servizi.

Sebbene ti consigliamo di abilitare un set di base di servizi di sicurezza all'interno dei tuoi account AWS CloudTrail, come Amazon GuardDuty e Amazon Macie, alla fine potresti voler estendere queste funzionalità per ottenere valore aggiunto dalle tue risorse di log. Sono disponibili numerosi strumenti per i partner, come quelli elencati nel nostro programma APN Security Competency. Potresti anche

voler scrivere le tue domande per effettuare ricerche nei log. Con l'ampio numero di servizi gestiti che AWS offre, questo non è mai stato così facile. Esistono molti AWS servizi aggiuntivi che possono aiutarti nelle indagini che non rientrano nell'ambito di questo paper, come Amazon Athena, Amazon OpenSearch Service, Amazon Quick, Amazon Machine Learning e Amazon EMR.

Appendice B: AWS risorse per la risposta agli incidenti

AWS pubblica risorse per assistere i clienti nello sviluppo di funzionalità di risposta agli incidenti. La maggior parte del codice e delle procedure di esempio è disponibile nell'archivio GitHub pubblico AWS esterno. Di seguito sono riportate alcune risorse che forniscono esempi di come eseguire la risposta agli incidenti.

Risorse del playbook

- [Framework for Incident Response Playbook](#): un framework di esempio che consente ai clienti di creare, sviluppare e integrare playbook di sicurezza in preparazione a potenziali scenari di attacco durante l'utilizzo dei servizi. AWS
- [Esempi di Incident Response Playbook](#): playbook che coprono gli scenari comuni affrontati dai clienti. AWS
- [AWS annuncia l'uscita di cinque workshop disponibili al pubblico](#).

Risorse forensi

- [Automated Incident Response and Forensics Framework](#): questo framework e questa soluzione forniscono un processo forense digitale standard, composto dalle seguenti fasi: contenimento, acquisizione, esame e analisi. Sfrutta le funzioni AWS λ per attivare il processo di risposta agli incidenti in modo automatizzato e ripetibile. Fornisce la separazione degli account per gestire le fasi di automazione, archiviare gli artefatti e creare ambienti forensi.
- [Automated Forensics Orchestrator for Amazon EC2](#): questa guida all'implementazione fornisce una soluzione self-service per acquisire ed esaminare i dati dalle istanze EC2 e dai volumi allegati per l'analisi forense nel caso in cui venga rilevato un potenziale problema di sicurezza. Esiste AWS CloudFormation un modello per implementare la soluzione.
- [Come automatizzare la raccolta forense dei dischi in AWS](#) questo AWS blog spiega come impostare un flusso di lavoro di automazione per acquisire le prove su disco da analizzare al fine di determinare la portata e l'impatto di potenziali incidenti di sicurezza. È incluso anche un AWS CloudFormation modello per implementare la soluzione.

Note

I clienti sono responsabili della propria valutazione indipendente delle informazioni contenute nel presente documento. Questo documento: (a) è solo a scopo informativo, (b) rappresenta le attuali offerte e pratiche di AWS prodotto, che sono soggette a modifiche senza preavviso, e (c) non crea alcun impegno o garanzia da parte delle sue affiliate, fornitori o AWS licenzianti. AWS i prodotti o i servizi sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite. Le responsabilità e le responsabilità dei AWS propri clienti sono regolate da AWS accordi e il presente documento non fa parte di, né modifica, alcun accordo tra AWS e i suoi clienti.

© 2024 Amazon Web Services, Inc. o società affiliate. Tutti i diritti riservati.

Cronologia dei documenti

La tabella seguente descrive importanti aggiunte alla documentazione di AWS Security Incident Response, a partire dal 1° gennaio 2026. Per ricevere notifiche sugli aggiornamenti della documentazione, puoi sottoscrivere il feed RSS.

Modifica	Descrizione	Data
Aggiorna la descrizione della politica per AWS Security Incident Response Triage Service Role Policy	Aggiorna la descrizione della policy per AWS Security Incident Response Triage Service Role Policy in modo da rispecchiare le modifiche che consentono al servizio di migliorare l'ottimizzazione del servizio e raccogliere informazioni per indagare su potenziali incidenti.	27 marzo 2026
Invia metadati	Sono state aggiunte istruzioni per l'invio di metadati tramite casi. Supporto AWS	27 marzo 2026
Invia le preferenze di contenimento	Sono state aggiunte istruzioni per l'invio delle preferenze di contenimento tramite casi. Supporto AWS	27 marzo 2026
Modello di contenimento StackSet	Aggiornato il modello di contenimento. StackSet CloudFormation	27 marzo 2026
Regione AWS Considerazioni chiarite per gli account degli amministratori delegati	È stato chiarito che, sebbene durante la configurazione iniziale venga designato un account amministratore delegato di AWS Security Incident Response in un	20 marzo 2026

unico account amministrativo, Regione AWS il servizio fornisce una copertura a livello dell'organizzazione per tutti gli account supportati. Regioni AWS

[Definire le preferenze relative alle azioni di contenimento](#)

È stata aggiornata la sezione delle preferenze per le azioni di contenimento in modo che corrisponda alle opzioni correnti.

19 marzo 2026

[Risposta proattiva e valutazione degli avvisi](#)

Sono stati rimossi i riferimenti al flusso di lavoro di risposta proattiva e valutazione degli avvisi come facoltativi.

3 marzo 2026

[Cronologia delle risposte](#)

Cronologia di risposta aggiornata per specificare lo SLO di 15 minuti per il riconoscimento del caso e 5 giorni lavorativi per la risposta del cliente prima della chiusura del caso.

24 febbraio 2026

[Migliori pratiche di comunicazione](#)

È stata aggiornata la tempistica di chiusura dei casi per specificare 5 giorni lavorativi per la risposta dei clienti alle richieste di informazioni critiche.

24 febbraio 2026

[AWS CLI riferimento aggiunto in Interacting with Security Incident Response utilizzando AWS CloudShell](#)

È stato aggiunto un collegamento al AWS Command Line Interface Reference for AWS Security Incident Response.

24 febbraio 2026

Matrice RACI	«Autorizza azioni di contenimento CIRT» è stato aggiornato a «Autorizza azioni di contenimento» nella matrice RACI.	13 febbraio 2026
Preferenze di contenimento	Opzioni di preferenza di contenimento aggiornate da «Nessuna azione di contenimento», «Contenimento con approvazione» e «Contenimento automatico» a «Approvazione richiesta», «Contenimento confermato» e «Contenimento sospetto» con descrizioni riviste.	13 febbraio 2026
Dopo l'implementazione della soluzione Security Incident Response	È stato aggiunto un collegamento alla demo AWS di Security Incident Response: nuove integrazioni e abbonamento a livello di OU.	4 febbraio 2026
Monitoraggio e indagine	È stato aggiunto un contenuto rivisto all'introduzione e alle sottosezioni di questa pagina.	4 febbraio 2026
Rileva e analizza	È stato aggiunto un contenuto rivisto all'introduzione e alle sottosezioni di questa pagina.	4 febbraio 2026
Contenere	È stato aggiunto contenuto rivisto a questa pagina.	4 febbraio 2026

Agente investigativo AI

È stato aggiunto l'informazione sull'uso dei dati dei clienti a questa pagina. Dichiarazione di non responsabilità: Al Investigative Agent non utilizza i dati dei clienti per la formazione dei modelli e non condivide i dati dei clienti con terze parti.

4 febbraio 2026

Modifica	Descrizione	Data
Annulla l'iscrizione	Pagina di annullamento dell'iscrizione aggiornata per indicare che l'iscrizione e il servizio termineranno immediatamente dopo l'annullamento e non alla fine del ciclo di fatturazione.	20 novembre 2025
AWS Policy gestite	Sono stati aggiunti casi di aggiornamento, creazione di commenti sui casi, elenca casi, elenca commenti sui casi all'elenco delle azioni fornite dal servizio.	19 novembre 2025
Uso di ruoli collegati ai servizi	Sono stati aggiunti casi di aggiornamento, creazione di commenti sui casi, elenca casi, elenca commenti sui casi all'elenco delle azioni fornite dal servizio.	19 novembre 2025
Preferenze di comunicazione	Creata e aggiornata la sezione Preferenze di comunicazione	12 novembre 2025

Modifica	Descrizione	Data
	<u>aggiunte per la documentazione sulle nuove funzionalità.</u>	

Modifica	Descrizione	Data
Agiunte e aggiornamenti della guida all'onboarding	<p>Creata e aggiornata È stata aggiunta una guida all'imbarco che include le seguenti sezioni</p> <p>Aggiunta la sezione Enable Security Incident Response.</p> <p>È stata aggiunta la sezione Autorizza i tecnici di Security Incident Response a eseguire azioni di contenimento delle minacce.</p> <p>È stata aggiunta la sezione Post Deployment of Security Incident Response.</p> <p>È stata aggiunta la sezione Aggiorna l'Incident Response Team.</p> <p>È stata aggiunta la sezione GuardDuty Risultati e regole di soppressione.</p> <p>Aggiunta la EventBridge sezione Amazon.</p> <p>È stata aggiunta la sezione Integrazioni e flussi di lavoro con strumenti esterni.</p> <p>È stata aggiunta la sezione External Tooling Workflow.</p> <p>Aggiunta l'Appendice A: sezione Punti di contatto.</p>	12 novembre 2025

Modifica	Descrizione	Data
Aggiornamenti sulla conformità e sulla lingua di fatturazione	<p>Aggiornamento: è stata rimossa la dichiarazione secondo cui AWS Security Incident Response non è coperto da alcun framework . AWS Security Incident Response è ora coperto da HITRUST, ma ne verranno aggiunti altri in futuro.</p> <p>Visibilità e controllo aggiornati per aggiungere Security Incident Response AWS</p> <p>Aggiornamento Annulla iscrizione per chiarire i periodi di fatturazione del servizio.</p> <p>È stato aggiunto un video a Getting Started che fornisce un contesto aggiuntivo per le attività tipiche da iniziare a utilizzare AWS Security Incident Response.</p>	15 agosto 2025

Modifica	Descrizione	Data
Aggiornato: AWSSecurityIncidentResponseServiceRolePolicy	<p>La politica ora include due nuove azioni "organizations:DescribeAccount" "organizations:ListDelegatedAdministrators" e una nuova condizione:</p> <pre data-bbox="594 569 1024 1003">"Condition": { "StringEquals": { "aws:ResourceAccount": "\${aws:PrincipalAccount}" } }</pre>	TBD

Modifica	Descrizione	Data
Aggiornamento della funzionalità: iscrizione a unità organizzative specifiche (OUs) o all'intera organizzazione AWS	<p>I pannelli di aiuto nell'interfaccia utente sono stati aggiornati per riflettere un aggiornamento relativo alla sottoscrizione a unità organizzative specifiche (OUs) o all'intera AWS organizzazione.</p> <p>Creazione di una nuova pagina per la gestione dell'appartenenza alle unità organizzative () OUs</p> <p>Pagine correlate AWS Organizations aggiornate per riflettere le nuove funzionalità di gestione delle unità organizzative.</p>	7 agosto 2025
Service Quotas aggiornate	La pagina Service Quotas è stata aggiornata per guidare gli utenti verso la General Reference Guide for Security Incident Response (Guida di riferimento AWS generale per gli endpoint e le quote AWS di Security Incident Response)	7 agosto 2025

Modifica	Descrizione	Data
<p>Aggiornamenti relativi al feedback degli utenti</p>	<p>Aggiunti collegamenti ipertestuali per il servizio ai casi di risposta agli incidenti AWS di sicurezza</p> <p>Aggiornamento in base alla Computer Security Incident Handling Guide SP 800-61 r3 per la Security Technical Guide</p>	<p>7 agosto 2025</p>
<p>Aggiunta una pagina per EventBridge l'integrazione di Amazon con AWS Security Incident Response.</p>	<p>Nuova sezione di contenuti per descrivere come Amazon si EventBridge integra in AWS Security Incident Response.</p>	<p>26 giugno 2025</p>
<p>Aggiornamenti a SLR che aggiungono autorizzazioni ai diritti al servizio di supporto.</p>	<p>AWSSecurityIncidentResponseTriageServiceRolePolicy è stato aggiornato per aggiungere security-ir:GetMembership, security-ir:, security-ir:, guardduty:, guardduty:ListMemberships, guardduty: e guardduty: UpdateCase e guardduty : permissions. guardduty: ListFilters è stato aggiunto per facilitare la gestione UpdateFilter dei filtri di archiviazione automatica negli account DeleteFilter delegati. GetAdministratorAccount GetAdministratorAccount GuardDuty</p>	<p>02 giugno 2025</p>

Modifica	Descrizione	Data
Aggiornamenti delle risorse.	Risorse aggiornate https://docs.aws.amazon.com/security-ir/latest/userguide/appendix-b-incident-response-resources.html #playbook -resources per riflettere i workshop attivi disponibili per i clienti.	23 maggio 2025
Il servizio supporta la lingua giapponese.	Configurazioni supportate e aggiornate per identificare il supporto per la lingua giapponese nell'ora locale del Giappone. L'inglese è supportato a livello globale.	13 maggio 2025

Modifica	Descrizione	Data
Aggiornamenti dei contenuti e feedback dei clienti.	<p>È stata aggiunta una nota a https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account-.html per indicare un'attività aggiuntiva quando si utilizza un account amministratore delegato come parte della configurazione.</p> <p>È stata aggiornata l'esperienza del cliente quando si lavora con un caso generato dal servizio e su Detect and Analyze.</p> <p>Dettagli aggiornati sulla cancellazione dell'account per fornire maggiore chiarezza sulle implicazioni di fatturazione derivanti dall'annullamento di un'iscrizione.</p>	9 maggio 2025
Aggiunta di tre nuove regioni supportate.	Sono state aggiunte tre nuove regioni a https://docs.aws.amazon.com/security-ir/latest/userguide/supported-configs.html . Mumbai, Parigi e San Paolo.	7 maggio 2025

Modifica	Descrizione	Data
Aggiornato: aggiornamenti dei commenti dei clienti sui documenti.	<p data-bbox="591 205 959 338">Gli errori di ortografia e grammatica su più pagine sono corretti.</p> <p data-bbox="591 384 1013 701">https://docs.aws.amazon.com/en_us/Sicurezza aggiornata: ir/latest/userguide/organizations_permissions.html per riflettere accuratamente security-ir come prefisso del servizio.</p> <p data-bbox="591 747 1013 968">È stata aggiunta una nota a https://docs.aws.amazon.com/security-ir/latest/userguide/source-containment.html relativa a Route53 e DNS.</p>	7 febbraio 2025

Modifica	Descrizione	Data
<p>Aggiornato: aggiornamenti dai commenti dei clienti sui documenti.</p>	<p>Aggiornato https://docs.aws.amazon.com/security-ir/latest/userguide/setup-monitoring-and-investigation-workflows.html al modello stackset.</p> <p>Voci corrette da triage.security-ir.com a triage.amazonaws.com</p> <p>È stata aggiunta una nota sulle connessioni tracciate per <code>2Reversible</code> su https://docs.aws.amazon.com/security-ir/latest/userguide/contain</p> <p>Risolto il problema con il collegamento interrotto su https://docs.aws.amazon.com/security-ir/latest/userguide/managing-associated-accounts.html.</p> <p>È stata aggiunta una definizione per l'account di iscrizione in https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account.html.</p> <p>È stata aggiunta una nota di chiarimento a https://docs.aws.amazon.com/en_us/security-ir/latest/userguid</p>	<p>20 dicembre 2024</p>

Modifica	Descrizione	Data
	e/using - service-linked-roles .html per AWS Organizations gli account di gestione.	

Modifica	Descrizione	Data
<p>Aggiornato: aggiornamenti dai commenti dei clienti sui documenti.</p>	<p>Sono stati rimossi più duplicati AWS AWS nel testo.</p> <p>Collegamenti interrotti fissi su https://docs.aws.amazon.com/security-ir/latest/userguide/sir_tagging.html and https://docs.aws.amazon.com/security-ir/latest/userguide/service-name-info-in-cloudtrail.html.</p> <p>Aggiornamenti https://docs.aws.amazon.com/security-ir/latest/userguide/containers.html. È stato rimosso il > dal primo paragrafo. Ha sostituito AWSSupport-ContainEC2Reversible con AWSSupport-ContainEC2Instance. Sostituito con. AWSSupport-ContainIAMReversible AWSSupport-ContainIAMPrincipal Sostituito AWSSupport-ContainS3Reversible con AWSSupport-ContainS3Resource.</p> <p>Formattazione aggiornata su security-ir.html https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/issues</p> <p>Quando si dice ai clienti di contattare la risposta agli incidenti di sicurezza tramite un ticket di assistenza, https://docs.aws.amazon.com/</p>	<p>10 dicembre 2024</p>

Modifica	Descrizione	Data
	<p>security-ir/ latest/userguide/understand - response-teams-and-support .html ora offre opzioni da selezionare nei moduli di supporto.</p> <p>CloudWatch Eventi rimossi e sostituiti con EventBridge on https://docs.aws.amazon.com/security-ir/latest/userguide/logging-and-events.html.</p> <p>Aggiornamenti grammaticali su https://docs.aws.amazon.com/security-ir/latest/userguide/technique-access-containment.html.</p> <p>Data di pubblicazione rimossa da https://docs.aws.amazon.com/security-ir/latest/userguide/security-incident-response-guide.html, sostituita dagli aggiornamenti in questa tabella.</p>	
<p>Aggiornamento: politiche AWS gestite e ruoli collegati ai servizi.</p>	<p>Aggiornamenti alle politiche gestite e ai ruoli collegati ai servizi.</p>	<p>1 dicembre 2024</p>
<p>Avvio del servizio</p>	<p>Documenti di servizio iniziali per il lancio del servizio a re:Invent 2024</p>	<p>1 dicembre 2024</p>

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.