AWS Guida dell'utente di Security Incident Response

Version December 1, 2024

AWS Guida dell'utente di Security Incident Response:

Table of Contents

Che cos'è AWS la risposta agli incidenti di sicurezza? 1
Configurazioni supportate 1
Riepilogo delle funzionalità 2
Monitoraggio e indagine 2
Semplifica la risposta agli incidenti 2
Soluzioni di sicurezza self-service 3
Dashboard per la visibilità 3
Posizione di sicurezza 3
Assistenza rapida 3
Preparazione e prontezza 3
Concetti e terminologia 4
Nozioni di base 6
Seleziona un account di iscrizione 6
Imposta i dettagli dell'iscrizione 7
Associa gli account a AWS Organizations 8
Imposta flussi di lavoro proattivi di risposta e valutazione degli avvisi 8
Attività dell'utente 10
Dashboard 10
Gestire il mio Incident Response Team 10
Associazione dell'account a AWS Organizations 11
Monitoraggio e indagine 2
Preparazione 12
Rileva e analizza 12
Contenere 15
Sradicare 18
Ripristino 18
Pubblica il rapporto sull'incidente 19
Casi 20
Crea un caso AWS supportato 20
Crea un caso autogestito 22
Rispondere a un caso generato AWS 23
Gestione dei casi 24
Modifica dello stato del caso 24
Cambiare il resolver 25
Attività 25

Modifica di un caso ... 25
Comunicazioni ... 26
Autorizzazioni ... 26
Allegati ... 27
Tag ... 28
Attività del caso ... 28
Chiusura di un caso ... 28
Lavorare con gli stackset AWS CloudFormation ... 29
Annulla iscrizione ... 35
Etichettatura delle risorse AWS di Security Incident Response ... 37
Usando AWS CloudShell ... 38
Ottenere le autorizzazioni per IAM AWS CloudShell ... 38
Interazione con Security Incident Response utilizzando AWS CloudShell ... 39
CloudTrail registri ... 40
Informazioni sulla risposta agli incidenti di sicurezza in CloudTrail ... 40
Informazioni sulle voci dei file di registro di Security Incident Response ... 42
Gestione degli account con AWS Organizations ... 45
Considerazioni e raccomandazioni ... 45
Accesso attendibile ... 46
Autorizzazioni necessarie per designare un account amministratore delegato di Security Incident Response ... 48
Designazione di un amministratore delegato Security Incident Response AWS ... 49
Aggiungere membri a AWS Security Incident Response ... 51
Rimozione di membri da AWS Security Incident Response ... 52
Risoluzione dei problemi ... 53
Problemi ... 53
Errori ... 53
Support ... 54
Sicurezza ... 56
Protezione dei dati nella risposta agli incidenti AWS di sicurezza ... 56
Crittografia dei dati ... 57
Riservatezza del traffico Internet ... 58
Traffico tra servizio e applicazioni e client locali ... 58
Traffico tra risorse AWS nella stessa Regione ... 58
Identity and Access Management ... 59
Autenticazione con identità ... 60
Come funziona AWS Security Incident Response con IAM ... 63

Risoluzione dei problemi AWS di identità e accesso al Security Incident Response 71
Utilizzo dei ruoli di servizio 73
Uso di ruoli collegati ai servizi 73
AWSServiceRoleForSecurityIncidentResponse 74
AWSServiceRoleForSecurityIncidentResponse_Triage 75
Regioni supportate per SLRs 76
AWS Policy gestite 77
politica gestita: AWSSecurityIncidentResponseServiceRolePolicy 78
politica gestita: AWSSecurityIncidentResponseAdmin 78
politica gestita: AWSSecurityIncidentResponseReadOnlyAccess 79
politica gestita: AWSSecurityIncidentResponseCaseFullAccess 80
politica gestita: AWSSecurityIncidentResponseTriageServiceRolePolicy 80
Aggiornamenti SLRs e politiche gestite 81
Risposta agli incidenti 83
Convalida della conformità 84
Registrazione e monitoraggio in AWS Security Incident Response 85
Resilienza 85
Sicurezza dell'infrastruttura 86
Analisi della configurazione e delle vulnerabilità 86
Prevenzione del confused deputy tra servizi 86
Service Quotas (Quote di Servizio) 88
AWS Risposta agli incidenti di sicurezza 88
AWS Guida tecnica sulla risposta agli incidenti di sicurezza 90
Sintesi 90
Sei tu Well-Architected? 90
Introduzione 91
Prima di iniziare 91
AWS panoramica della risposta agli incidenti 92
Preparazione 98
Persone 99
Processo 103
Tecnologia 110
Riepilogo degli elementi di preparazione 117
Operazioni 122
Rilevamento 123
Analisi 127
Contenimento 132

Rimozione 138
Ripristino 140
Conclusioni 141
Attività post-incidente 142
Stabilire un quadro per imparare dagli incidenti 143
Stabilisci metriche per il successo 144
Usa indicatori di compromesso 148
Istruzione e formazione continue 149
Conclusioni 149
Collaboratori 150
Appendice A: Definizioni delle funzionalità cloud 150
Registrazione ed eventi 150
Visibilità e avvisi 152
Automazione 155
Archiviazione sicura 155
Funzionalità di sicurezza future e personalizzate 156
Appendice B: risorse per la risposta AWS agli incidenti 156
Risorse del playbook 157
Risorse forensi 157
Note 157
Cronologia dei documenti 159
..... clxiii

Cos'è la risposta agli incidenti di AWS sicurezza?

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 acquisizioni di account, violazioni di dati e attacchi ransomware.

AWS Security Incident Response valuta i risultati, analizza gli eventi di sicurezza e gestisce i casi che richiedono l'attenzione immediata dell'utente. Inoltre, hai accesso al AWS Customer Incident Response Team (CIRT), che esaminerà 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 si integra con altri servizi di AWS rilevamento e risposta, guidandoti 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 linguistiche e regionali:

- Lingua: AWS Security Incident Response è disponibile in inglese.
- AWS Regioni supportate:

  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)
  - US West (Oregon)
  - Stati Uniti orientali (Virginia)
  - UE (Francoforte)

- UE (Irlanda)
- UE (Londra)
- UE (Stoccolma)
- Asia Pacifico (Singapore)
- Asia Pacifico (Seoul)
- Asia Pacifico (Sydney)
- Asia Pacifico (Tokyo)
- Canada (Centrale)

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 practice di sicurezza, AWS consiglia di abilitarla GuardDuty in tutte le AWS regioni supportate. 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 di sicurezza provenienti da Amazon GuardDuty e dalle integrazioni di terze parti AWS Security Hub, riducendo il numero di avvisi di sicurezza che il team deve analizzare. Configura le regole di soppressione in base al tuo ambiente per ridurre gli avvisi a bassa priorità 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 prevede 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

Connettiti con AWS il Customer Incident Response Team (CIRT) per indagare, contenere e ricevere indicazioni su come 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 servizio AWS Security Incident Response e come funziona.

Ambito di applicazione: AWS Security Incident Response è conforme alla guida 800-61 del National Institute of Standards and Techology (NIST) 800-61 Computer Security Incident Handling, che fornisce un approccio coerente alla gestione degli eventi di sicurezza in base 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 Portale del servizio Security Incident Response: un portale self-service che consente di avviare e gestire casi di eventi di sicurezza. Comunicazione e reportistica continue agevolate dal sistema di ticketing, 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 dalle precedenti collaborazioni per potenziare le capacità di rilevamento, i processi investigativi e le azioni correttive. AWS Security Incident Response si attiene up-to-date inoltre alle più recenti minacce alla sicurezza e alle migliori pratiche per affrontare le sfide di sicurezza in continua evoluzione.

Evento di sicurezza informatica: qualsiasi evento osservabile in un sistema o in una rete che viola o minaccia di violare le politiche di sicurezza, le politiche di utilizzo accettabile o le pratiche di sicurezza standard.

Incident Response Team: un gruppo di persone che forniscono supporto durante eventi di sicurezza attivi. Per i casi AWS supportati, si tratta del AWS Customer Incident Response Team (CIRT).

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: strumenti di AWS Security Incident Response 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: AWS Security Incident Response esamina 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 offre un'unica dashboard centralizzata AWS Management Console per gestire tutte le attività di AWS Security Incident Response.

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

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

Indice

- 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

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 iscrizione a AWS Security Incident Response allo stesso account che hai abilitato per servizi come Amazon GuardDuty e AWS Security Hub.

Hai due opzioni per selezionare il tuo account di iscrizione a AWS Security Incident Response 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 amministrative e la gestione dei casi di AWS Security Incident Response 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.

Usa l'account attualmente connesso: selezionando questo account, l'account corrente diventerà l'account di iscrizione centrale per l'iscrizione a AWS Security Incident Response. 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 delle autorizzazioni sufficienti per amministrare AWS Security Incident Response.

Fai riferimento a Aggiungere e rimuovere le autorizzazioni di IAM identità per i passaggi specifici per aggiungere le autorizzazioni.

Fai riferimento alle politiche gestite AWS di Security Incident Response.

Per verificare IAM le autorizzazioni, puoi seguire questi passaggi:

- Verifica la IAM politica: esamina la IAM politica 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 politica 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 AWS CLI oSDK: puoi usare l'interfaccia a riga di AWS Command Line Interface comando (CLI) o un altro AWS SDK nel tuo linguaggio di programmazione preferito per testare le autorizzazioni. Ad esempio, con AWS Command Line Interface, è possibile 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 IAM policy: il simulatore di IAM policy è uno strumento che ti permette di testare IAM le policy 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.

- Facoltativamente, puoi selezionare un nome per questo abbonamento.
- È necessario fornire un contatto principale e secondario come parte del flusso di lavoro per la creazione dell'iscrizione. Questi contatti vengono automaticamente inclusi nel 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

La tua iscrizione dà diritto alla copertura su tutti i link Account AWS in AWS Organizations. Gli account associati verranno aggiornati automaticamente non appena gli account vengono aggiunti o rimossi dall'organizzazione.

Imposta flussi di lavoro di risposta proattiva e valutazione degli avvisi

Il flusso di lavoro di risposta proattiva e valutazione degli avvisi è una funzionalità opzionale da abilitare all'interno dell'organizzazione per il monitoraggio dei servizi di sicurezza abilitati. Seleziona l'interruttore accanto alla funzione da abilitare.

Se riscontri problemi di onboarding, crea una AWS Support richiesta per ricevere 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.

Risposta proattiva e triaging degli avvisi: AWS Security Incident Response monitora e analizza gli avvisi generati dalle integrazioni di Amazon e GuardDuty Security 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 funziona AWS Security Incident Response con Amazon GuardDuty AWS Security Hub, consulta la sezione Rileva e analizza della guida per l'utente.

Questa funzionalità consente a AWS Security Incident Response di monitorare e analizzare i risultati relativi a tutti gli account e alle attività supportate Regioni AWS nell'organizzazione. Per facilitare questa funzionalità, AWS Security Incident Response crea automaticamente un ruolo collegato al servizio in tutti gli account membri 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.

Contenimento: in caso di incidente di sicurezza, Security Incident Response può eseguire azioni di contenimento per mitigare rapidamente l'impatto, come l'isolamento degli host compromessi o la rotazione delle AWS credenziali. Per impostazione predefinita, Security Incident Response non abilita le funzionalità di contenimento. 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

- Dashboard
- Gestire il mio Incident Response Team
- Associazione dell'account a AWS Organizations
- Monitoraggio e indagine
- Casi
- Gestione dei casi
- Lavorare con gli AWS CloudFormation stackset
- Annulla iscrizione

Dashboard

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

Seleziona questa opzione `View incident response team` per accedere ai dettagli dei tuoi colleghi addetti alla risposta agli incidenti.

Seleziona `proactive response` per identificare se la gestione degli avvisi è abilitata. Se non hai il `alert triaging` flusso di lavoro abilitato, puoi monitorarne lo stato e scegliere di `Proactive Response` abilitarlo.

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 l'iscrizione e i casi. È possibile utilizzare policy AWS gestite per AWS Security Incident Response per 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 sui seguenti eventi:

- Caso (creazione, eliminazione, aggiornamento)
- Commento (creazione, eliminazione, aggiornamento)
- Allegato (creazione, eliminazione, aggiornamento)
- Iscrizione (creazione, aggiornamento, annullamento, ripresa)

Associazione dell'account a AWS Organizations

Quando attivi AWS Security Incident Response, l'iscrizione verrà creata e allineata alla tua AWS Organizations. Tutti gli account all'interno delle tue Organizations sono allineati alla tua iscrizione a AWS Security Incident Response.

Per maggiori dettagli, consulta Gestire gli account AWS Security Incident Response con AWS Organizations.

Monitoraggio e indagine

AWS Security Incident Response esamina e classifica gli avvisi di sicurezza di Amazon GuardDuty AWS Security Hub, quindi configura le regole di soppressione in base al tuo ambiente per prevenire avvisi non necessari. Il AWS CIRT team analizza i risultati non classificati e si occupa rapidamente

della situazione e lo guida per contenere rapidamente i potenziali problemi. Se lo desideri, puoi concedere a AWS Security Incident Response l'autorizzazione a implementare azioni di contenimento per tuo conto.

AWS Security Incident Response si allinea alla NIST 800-61r2 Computer Security Event Handling Guide for Security Event Response. Allineandosi a questo standard di settore, AWS Security Incident Response offre 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 il servizio AWS Security Incident Response identifica un avviso di sicurezza o si richiede assistenza in materia di sicurezza, effettua un'indagine. AWS CIRT Il team raccoglie gli eventi di registro e i dati di servizio, ad esempio GuardDuty avvisi, classificazioni e analizza tali dati, esegue attività di correzione e contenimento e fornisce report post-incidente.

Indice

- Preparazione
- Rileva e analizza
- Contenere
- Sradicare
- Ripristino
- Rapporto post-incidente

Preparazione

Il team AWS Security Incident Response 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

AWS Security Incident Response monitora, valuta, analizza i risultati di sicurezza di Amazon GuardDuty e le integrazioni. AWS Security Hub Altre azioni che possono migliorare in modo significativo la portata e l'efficacia delle funzionalità di monitoraggio e indagine di AWS Security Incident Response includono:

Abilitazione delle fonti di rilevamento supportate

> **Note**
>
> AWS I costi del servizio Security Incident Response non includono l'utilizzo e altri costi e tariffe associati alle fonti di rilevamento o all'uso di altri AWS servizi supportate. Consulta le pagine delle singole funzionalità o dei servizi per i dettagli sui costi.

Amazon GuardDuty

GuardDuty è un servizio di rilevamento delle minacce che monitora, analizza ed elabora continuamente le fonti di dati e i registri presenti nell'ambiente. AWS GuardDuty L'abilitazione non è necessaria per utilizzare AWS Security Incident Response; tuttavia, per utilizzare la funzione di risposta proattiva e di triaging degli avvisi, è GuardDuty necessario abilitare Amazon.

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 a 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

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

Per abilitare l'integrazione di Security Hub with Organizations, consulta la Guida per AWS Security Hub l'utente.

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

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

- CrowdStrike — CrowdStrike Falco
- Merletto — Merletto
- Trend Micro — Cloud One

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

Analisi dei risultati.

AWS Il team di AWS CIRT assistenza e di automazione di Security Incident Response analizzerà tutti i risultati degli strumenti supportati. Inizieremo a conoscere il tuo ambiente comunicando con te utilizzando AWS Support Cases. Ad esempio, quando abbiamo bisogno di capire se un risultato è un comportamento previsto o se deve essere trasformato in un incidente. Man mano che acquisiremo ulteriori informazioni dal vostro ambiente, personalizzeremo il servizio e ridurremo il numero di comunicazioni.

Segnalazione di un evento.

È possibile segnalare un evento di sicurezza tramite il portale del servizio AWS Security Incident Response. 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 modelli anomali. La collaborazione e la comprensione dell'ambiente in uso accelerano questa analisi.

Comunica.

AWS Security Incident Response ti tiene informato durante le indagini coinvolgendo i tuoi contatti di sicurezza tramite il ticket dell'evento. Più membri del team possono supportare il tuo evento, tutti utilizzando il ticket dell'evento per ricevere contenuti e aggiornamenti forniti dal cliente. AWS

La comunicazione può includere notifiche automatiche quando viene generato un avviso di sicurezza, comunicazioni durante l'analisi degli eventi, creazione di call bridge, analisi continua di elementi come i file di registro e invio all'utente dei risultati delle indagini durante l'evento di sicurezza.

AWS Security Incident Response utilizza due diversi tipi di casi per comunicare con l'utente: Support per le comunicazioni in uscita per avvisare l'utente di un evento e i casi di AWS Security Incident Response per comunicare su un caso che ci avete presentato.

AWS Casi di supporto: il servizio utilizzerà AWS Support Cases per comunicare con i team. Creeremo casi di supporto per ciascuno dei casi Account AWS in cui viene generato il risultato. Questo approccio facilita la comunicazione con i diversi team responsabili dei carichi di lavoro specifici, in quanto avranno una maggiore conoscenza degli eventi che si verificano nelle loro aree di responsabilità.

AWS Casi di risposta agli incidenti di sicurezza: se stabiliamo che una scoperta deve essere trasformata in un incidente di sicurezza, creeremo un caso di risposta agli incidenti di sicurezza. AWS Ciò garantisce che i problemi di sicurezza critici ricevano il livello di attenzione e risposta appropriato.

Interagendo attivamente con queste comunicazioni e fornendo risposte tempestive, puoi aiutare il servizio AWS Security Incident Response a:

- Comprendi meglio il tuo ambiente e i comportamenti previsti.
- Riduci i falsi positivi nel tempo.
- Migliora l'accuratezza e la pertinenza degli avvisi.
- Garantisci una risposta rapida a veri incidenti di sicurezza.
- Ricorda che l'efficacia del servizio AWS Security Incident Response migliora con la collaborazione, portando a un AWS ambiente monitorato più sicuro ed efficiente.

Contenere

AWS Security Incident Response collabora con te per contenere gli eventi. Puoi configurare un ruolo di servizio per AWS Security Incident Response in modo che intraprenda azioni automatiche e manuali sul tuo account in risposta agli avvisi. Puoi anche eseguire il contenimento da solo o in collaborazione con le tue relazioni con terze parti utilizzando SSM i documenti.

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.

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:

- EC2Contenimento: l'automazione del `AWSSupport-ContainEC2Instance` contenimento esegue un contenimento di rete reversibile di un'EC2istanza, lasciandola intatta e funzionante, ma isolandola da qualsiasi nuova attività di rete e impedendole di comunicare con le risorse interne ed esterne all'utente. 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 SSM documento. Ulteriori informazioni sono disponibili nella sezione relativa al contenimento dei sorgenti della guida tecnica al servizio.

- IAMContenimento: l'automazione del `AWSSupport-ContainIAMPrincipal` contenimento esegue un contenimento di rete reversibile di un IAM utente o di un ruolo, lasciando l'utente o il ruolo internoIAM, 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.

> **Important**
>
> AWS Security Incident Response non abilita le funzionalità di contenimento per impostazione predefinita, per eseguire queste azioni di contenimento, è necessario prima concedere le autorizzazioni necessarie al servizio utilizzando i ruoli. È possibile creare questi ruoli singolarmente per account o per l'intera organizzazione utilizzando gli AWS CloudFormation stackset, che creano i ruoli richiesti.

AWS Security Incident Response ti incoraggia a prendere in considerazione strategie di contenimento per ogni tipo di evento importante che rientrino nella tua 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 il rischio e concedere il tempo necessario per definire e implementare una strategia di contenimento più efficace.

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

- Strategia di contenimento
  - AWS Security Incident Response è in grado di 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?
    - Se sì, 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
  - Sono state create copie di backup dei sistemi interessati 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.

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 AWS CIRT collaboreremo con voi per valutare le azioni necessarie.

Considera i seguenti aspetti:

- È possibile reimpostare l'immagine del sistema e renderlo più sicuro 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 stati 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?

Rapporto 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 servizio AWS Security Incident Response invierà report mensili al punto di contatto principale di ogni cliente tramite e-mail. I report verranno consegnati in un PDF formato che utilizza le metriche descritte di seguito. I clienti riceveranno un rapporto per persona. AWS Organizations

Metriche del caso

- Casi creati
  - Nome 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 analizzati manualmente
  - Unità: numero
  - Descrizione: Il numero di risultati con indagine manuale eseguiti.
- Indagini archiviate
  - Unità: numero
  - Descrizione: il numero di indagini manuali che hanno prodotto falsi positivi e inviate per l'archiviazione
- Le indagini si sono intensificate
  - 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 gestiti autonomamente.

Crea un caso AWS supportato

È possibile creare un caso AWS supportato dal AWS Security Incident Response, dalAPI, o dal AWS Command Line Interface. AWS i casi supportati consentono di ricevere assistenza dal AWS Customer Incident Response Team (CIRT).

> **Note**
>
> AWS CIRTrisponderà al tuo caso entro 15 minuti. Il tempo di risposta si riferisce alla prima risposta di AWS CIRT. Faremo ogni ragionevole sforzo per rispondere alla tua richiesta iniziale entro questo periodo di tempo. Questo tempo di risposta non si applica alle risposte successive.

L'esempio seguente riguarda l'uso della console.

1. Accedi alla AWS Management Console. Aprire la console Security Incident Response all'indirizzo https://console.aws.amazon.com/security-ir/.

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: le indagini consentono di ottenere assistenza in caso di incidenti di sicurezza percepiti, ma AWS CIRT possono essere utili anche nelle indagini di log dive e, in secondo luogo, di conferma della risposta agli incidenti.
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, il team di risposta agli incidenti AWS CIRT e il team di risposta agli incidenti vengono immediatamente informati.

Crea un caso autogestito

Puoi creare un file autogestito dal AWS Security Incident Response, dalAPI, o dal. AWS Command Line Interface Questo tipo di caso DOESNOTcoinvolge il AWS CIRT. L'esempio seguente riguarda l'uso della console.

1. Accedi alla AWS Management Console. Aprire la console Security Incident Response all'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.

Risposta a un caso AWS generato

AWS Security Incident Response può creare una notifica o un caso in uscita in cui è necessario intervenire o venire a conoscenza di qualcosa che potrebbe influire sul proprio account o sulle proprie risorse. Ciò si verificherà solo se hai abilitato i flussi di lavoro di risposta proattiva e triaging degli avvisi abilitati come parte dell'abbonamento.

Queste notifiche verranno visualizzate in Center. Support La guida per Support l'utente contiene informazioni e passaggi dettagliati per l'aggiornamento, la risoluzione e la riapertura di questi casi.

Gestione dei casi

Indice

- Modifica dello stato del caso
- Modifica del resolver
- Attività
- Modifica di un caso
- Comunicazioni
- Autorizzazioni
- Allegati
- Tag
- Attività relative ai casi
- Chiusura di un caso

Modifica dello stato del caso

Un caso si troverà 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 SSM i documenti 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 dal risponditore. AWS CIRT

Modifica del 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 AWS CIRT. Una volta che avrai richiesto assistenza, non AWS potrai tornare a gestirla in modalità autogestita.

Attività

Un AWS CIRT soccorritore che si occupa del caso può richiedere azioni al tuo 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

Intervento da intraprendere quando un'azione del cliente è in sospeso:

- Richiesta di intervento in base a un nuovo commento per procedere con il 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:

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

- Titolo

- Descrizione

Solo per i casi AWS supportati:

Puoi modificare i campi aggiuntivi:

- Tipo di 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, ma AWS CIRT possono essere utili anche in fase di registrazione e, in secondo luogo, di conferma della risposta all'incidente (evento).
- 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 CIRTpossono aggiungere commenti per documentare le proprie attività quando lavorano su un caso. Diversi AWS CIRT soccorritori possono lavorare su un caso contemporaneamente. Sono rappresentati come AWS Responder all'interno del registro delle comunicazioni.

Autorizzazioni

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 AWS Management Console, puoi copiare il modello di politica di IAM autorizzazione e aggiungere questa autorizzazione a un utente o a un ruolo.

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

1. Copia la politica di IAM autorizzazione.
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 gestita AWS di Security Incident Response appropriata.
8. Scegli Aggiungi policy.

Allegati

I soccorritori possono aggiungere allegati a un caso per aiutare gli altri addetti alle operazioni di risposta agli incidenti 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 il 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 per la chiusura prima di essere chiuso definitivamente. Se chiudi prematuramente un caso con uno stato diverso da Pronto a chiudere, stai richiedendo che questa richiesta AWS CIRT smetterà di funzionare su questo AWS caso supportato.

Se il team di risposta agli incidenti è incaricato del soccorso, 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 gli AWS CloudFormation stackset

> **Important**
>
> AWS Security Incident Response non abilita le funzionalità di contenimento per impostazione predefinita, per eseguire queste azioni di contenimento, è necessario prima concedere le autorizzazioni necessarie al servizio utilizzando i ruoli. È possibile creare questi ruoli singolarmente per account o per l'intera organizzazione distribuendoli AWS CloudFormation StackSets, che creano i ruoli richiesti.

Puoi trovare istruzioni specifiche su come creare un set di stack con autorizzazioni gestite dal servizio.

Di seguito sono riportati gli stackset di modelli per creare i ruoli e. AWSSecurityIncidentResponseContainmentAWSSecurityIncidentResponseContainmentExecution

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for AWS Security Incident Response containment roles'

Resources:
  AWSSecurityIncidentResponseContainment:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainment
      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: AWSSecurityIncidentResponseContainmentPolicy
          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
 AWSSecurityIncidentResponseContainmentExecution.Arn,
                    'Condition': { 'StringEquals': { 'iam:PassedToService':
 'ssm.amazonaws.com' } },
                  },
                ],
```

```
            }
  AWSSecurityIncidentResponseContainmentExecution:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainmentExecution
      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: AWSSecurityIncidentResponseContainmentExecutionPolicy
          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': '*',
              },
            ],
        }
```

Annulla iscrizione

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

> **Important**
>
> Una volta annullata l'iscrizione, non sarà possibile visualizzare i dati storici dei casi. Le cancellazioni avvengono alla fine del ciclo di fatturazione. Se effettui l'annullamento durante il mese, l'abbonamento sarà disponibile fino alla fine del mese. Qualsiasi risorsa o indagine

che sia `Active` o `ready to close` verrà interrotta in seguito alla cancellazione definitiva dell'iscrizione alla fine del ciclo di fatturazione.

Important

Se ti iscrivi nuovamente al servizio, verrà creata una nuova iscrizione e le risorse relative ai casi disponibili durante l'iscrizione 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 il AWS Organizations API per rimuovere la designazione di amministratore delegato dall'account, l'iscrizione verrà interrotta immediatamente.

Etichettatura delle risorse AWS di 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 `stagee` 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 dell'accesso tramite tag nella Guida IAM per l'utente.

Per l'etichettatura, consulta il API riferimento AWS Security Incident Response.

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. AWS Management ConsoleÈ possibile eseguire AWS CLI comandi contro i AWS 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 AWS Management Console, 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 per IAM AWS CloudShell
- Interazione con Security Incident Response utilizzando AWS CloudShell

Ottenere le autorizzazioni per IAM AWS CloudShell

Utilizzando le risorse di gestione degli accessi fornite da AWS Identity and Access Management, gli amministratori possono concedere autorizzazioni agli IAM utenti 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 politica gestita. Una policy gestita da AWS è una policy autonoma che viene creata e amministrata da AWS. La seguente politica AWS gestita per CloudShell può essere allegata alle IAM identità:

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

Se si desidera limitare l'ambito delle azioni che un IAM utente può eseguire AWS CloudShell, è possibile creare una politica personalizzata che utilizzi la politica `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 i IAM criteri nella Guida per l'AWS CloudShell utente.

> **Note**
>
> La tua IAM identità richiede anche una politica che conceda l'autorizzazione a effettuare chiamate a Security Incident Response.

Interazione con Security Incident Response utilizzando AWS CloudShell

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

> **Note**
>
> Quando si utilizza AWS CLI 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

- Da AWS Management Console, puoi avviarlo 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

Registrazione delle API chiamate AWS Security Incident Response tramite 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 API chiamate per Security Incident Response come eventi. Le chiamate acquisite includono le chiamate dalla console Security Incident Response e le chiamate in codice alle API operazioni di 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 AWS Management Console sono multiregionali. È possibile creare un percorso basato su una o più regioni solo utilizzando la AWS CLI. La creazione di un percorso multiregionale è consigliata in quanto consente di registrare l'intera attività del proprio Regioni AWS account. Creando un percorso a singola regione, è possibile visualizzare solo gli eventi registrati nella Regione AWS del percorso. Per ulteriori informazioni sulla creazione di percorsi ,

consulta Creazione di un percorso per un Account AWS e Creazione di un percorso per un'organizzazione nella Guida per l'utente 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 SQL basate sui tuoi eventi. CloudTrail Lake converte gli eventi esistenti in JSON formato basato su righe in formato Apache. ORC ORCè un formato di archiviazione colonnare 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, vedete l'CloudTrail userIdentityelemento.

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 stack ordinata delle API chiamate 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": "AROA00000000000000000:user",
        "arn": "arn:aws:sts::123412341234:assumed-role/Admin/user",
        "accountId": "123412341234",
        "accessKeyId": "****",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA00000000000000000",
                "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 degli account AWS Security Incident Response 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 per AWS Security Incident Response. Questa azione 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 di AWS Security Incident Response con AWS Organizations
- Attivazione dell'accesso affidabile per AWS Account Management
- Autorizzazioni necessarie per designare un account amministratore delegato di Security Incident Response
- Designazione di un amministratore delegato per Security Incident Response AWS
- Aggiungere membri a AWS Security Incident Response
- Rimozione di membri da AWS Security Incident Response

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

Un account amministratore delegato di Security Incident Response è regionale.

> L'account amministratore delegato di Security Incident Response e gli account membro devono essere aggiunti tramite. AWS Organizations

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.

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

La gestione dell'organizzazione può essere l'account amministratore delegato di Security Incident Response. Tuttavia, le best practice di sicurezza AWS seguono il principio del privilegio minimo e sconsigliano 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, AWS Security Incident Response rimuove tutti gli account membro associati a questo account amministratore delegato di Security Incident Response. AWS Security Incident Response non sarà più abilitato per tutti questi account membro.

Attivazione dell'accesso affidabile per AWS Account Management

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 nell'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 IAM utente, assumere un IAM ruolo o accedere come utente root (scelta non consigliata) 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 dialogo Abilita accesso affidabile per AWS Security Incident Response, digita enable per confermarlo, quindi scegli Abilita accesso affidabile.

API/CLI

Per abilitare l'accesso affidabile per AWS Account Management

Dopo aver eseguito il comando seguente, è possibile utilizzare le credenziali dell'account di gestione dell'organizzazione per richiamare API le operazioni di gestione degli 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 nell'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'iscrizione a AWS Security Incident Response utilizzando l'amministratore delegato per. AWS Organizations Per informazioni su come vengono concesse queste autorizzazioni, vedere Utilizzo AWS Organizations con altri AWS servizi.

> **Note**
>
> AWS Security Incident Response abilita automaticamente la relazione di AWS Organizations fiducia quando si utilizza la console per la configurazione e la gestione. Se si utilizzaCLI/SDK, è necessario abilitarlo manualmente utilizzando E nableAWSService Access API to trust`security-ir.amazonaws.com`.

In qualità di AWS Organizations manager, prima di designare l'account amministratore delegato di Security Incident Response per la propria organizzazione, verifica di poter eseguire le seguenti azioni di AWS Security Incident Response: `sir:CreateMembership` e. `sir: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 politica 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 la tua AWS Organizations gestione come account amministratore delegato di Security Incident Response, anche il tuo account richiederà l'IAMazione:. `CreateServiceLinkedRole` Questa azione consente di inizializzare AWS Security Incident Response per la gestione. Tuttavia, verifica Considerazioni e consigli per l'utilizzo di AWS Security Incident Response con AWS Organizations prima di procedere con l'aggiunta delle autorizzazioni.

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

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

Designazione di un amministratore delegato per Security Incident Response AWS

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:

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

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

Se AWS Security Incident Response non 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 abilitare AWS Security Incident Response per l'account amministratore delegato di Security Incident Response appena designato.

Aggiungere membri a AWS Security Incident Response

Esiste una relazione individuale con AWS Organizations e la tua iscrizione a AWS Security Incident Response. Man mano che gli account vengono aggiunti (o rimossi) dalle tue Organizations, ciò si rifletterà negli account coperti per la tua iscrizione a AWS Security Incident Response.

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

Rimozione di membri da AWS Security Incident Response

Per rimuovere un account dalla tua iscrizione, segui le procedure per rimuovere un account membro da un'organizzazione.

Risoluzione dei problemi

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

An ERROR è lo 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
- Support

Problemi

Non invio di richieste dal contesto corretto.

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

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 IAM ruolo nel tuo account di amministratore delegato o di iscrizione al AWS Security Incident Response. Verifica inoltre che il ruolo abbia una IAM politica 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 al servizio AWS Security Incident Response

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`.

InternalServerException

Si è verificato un errore imprevisto durante l'elaborazione della richiesta. Riprova tra qualche minuto. Se il problema persiste, solleva un caso con Support.

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 IAM ruoliIDs, alle iscrizioni, ai casi, ai membri del team di risposta, ai casi, ai rispondenti ai casi, agli allegati dei casi e ai commenti sui casi.

ThrottlingException

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

Il IAM responsabile della API funzione in questione ha fatto troppe richieste 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 convalida e/o combinazione logica. Verifica che tutte le risorse siano ARNs complete e che i valori di testo soddisfino i vincoli di dimensione e formato indicati nella AWS Security Incident Response API Reference Guide. Verifica inoltre che siano consentiti eventuali aggiornamenti dei valori. Ad esempio, non è possibile modificare un caso da AWS supportato a autogestito.

Support

Se hai bisogno di ulteriore assistenza, contatta il Support 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 nella risposta agli incidenti AWS di sicurezza
- Riservatezza del traffico Internet
- Identity and Access Management
- Risoluzione dei problemi AWS di identità e accesso a Security Incident Response
- 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 nella risposta agli incidenti AWS di sicurezza

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 di mantenere il controllo sui 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 la sezione Privacy dei dati FAQ. Per informazioni sulla protezione dei dati in Europa, consulta il Modello di responsabilitàAWS condivisa e il post di GDPR blog sul AWS Security Blog.

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. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- UsaSSL/TLSper comunicare con AWS le risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e 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.
- FIPS140-3 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 consoleAPI, 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 messaggio URL a un server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali URL per convalidare la tua richiesta a quel server.

Crittografia dei dati

Indice

- Crittografia dei dati inattivi
- Crittografia in transito
- Gestione delle chiavi

Crittografia dei dati inattivi

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 in transito

I dati raccolti e accessibili da AWS Security Incident Response avvengono esclusivamente su un canale protetto da 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 dai clienti.

Riservatezza del traffico Internet

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 AWS Direct Connect connessione. Per ulteriori informazioni, consulta Che cos'è AWS Direct Connect? nella Guida per l'utente di AWS Direct Connect .

L'accesso a AWS Security Incident Response tramite la rete avviene tramite AWS publishedAPIs. I client devono supportare Transport Layer Security (TLS) 1.2. Consigliamo la TLS versione 1.3. I client devono inoltre supportare suite di crittografia con Perfect Forward Secrecy (PFS), come Ephemeral Diffie-Hellman () o Elliptic Curve Diffie-Hellman Ephemeral (). DHE 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 principal IAM, oppure è possibile utilizzare AWS Security Token Service (STS) per generare le credenziali di sicurezza temporanee per firmare le richieste.

Traffico tra risorse AWS nella stessa Regione

Un endpoint Amazon Virtual Private Cloud (AmazonVPC) 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 a AWS Security Incident Response e reindirizza le risposte aVPC. Per ulteriori informazioni, consulta gli VPCendpoint nella Amazon VPC User Guide.

Ad esempio, le politiche che è possibile utilizzare per controllare l'accesso dagli VPC endpoint, vedere Utilizzo delle IAM politiche per controllare l'accesso a DynamoDB.

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

Identity and Access Management

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

Indice

- Autenticazione con identità
- Come funziona AWS Security Incident Response con IAM

Pubblico

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

Amministratori della sicurezza

Si consiglia a questi utenti di utilizzare la policy AWSSecurityIncidentResponseFullAccessgestita 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 del team di risposta agli incidenti

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 gestite di AWS Security Incident Response.

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 IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Gli utenti di IAM Identity Center (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 () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Firmare AWS API le richieste nella Guida per l'IAMutente.

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'IAMutente.

AWS account (utente root)

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 8 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 l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'IAMutente.

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, si consiglia di utilizzare Identity Center. AWS IAM È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un set di utenti e gruppi nella propria fonte di identità per utilizzarli su tutti gli AWS account e le applicazioni. Per informazioni su IAM Identity Center, vedi Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center.

IAMutenti e gruppi

Un IAMutente 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 anziché creare IAM utenti 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 IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. er ulteriori informazioni, consulta PRuotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente. IAM

Un IAMgruppo è un'identità che specifica un insieme di utenti. IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile assegnare un nome a un gruppo IAMAdminse concedere a tale gruppo le autorizzazioni per IAM amministrare le risorse.

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 IAM utente (anziché un ruolo) nella Guida per l'IAMutente.

Ruoli IAM

Un IAMruolo 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 IAM ruolo nella Console di AWS gestione cambiando ruolo. È possibile assumere un ruolo chiamando un' AWS APIoperazione AWS CLI or o utilizzando un'operazione personalizzataURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere Utilizzo IAM dei ruoli nella Guida per l'IAMutente.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a un'identità federata, è necessario 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 informazioni sui ruoli per la federazione, consulta Creazione di un ruolo per un provider di identità di terze parti nella Guida per l'utente. IAM Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAMIdentity Center.
- Autorizzazioni IAM utente temporanee: un IAM utente o un ruolo può assumere IAM il ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni AWS servizi, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra i ruoli e le politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse tra account IAM nella Guida per l'utente. IAM
- Accesso tra servizi: alcuni AWS servizi utilizzano le funzionalità di altri servizi. AWS Ad esempio, quando effettui una chiamata in un servizio, è normale che quel 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 IAMruolo che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio da IAM. Per ulteriori informazioni, consulta Creazione di un ruolo per delegare le autorizzazioni a un servizio AWS nella IAMGuida per l'utente.

- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un servizio. AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nell' AWS account e sono di proprietà del servizio. Un amministratore IAM può visualizzare, ma non modificare le autorizzazioni dei ruoli collegati ai servizi.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e che effettuano AWS CLI o effettuano AWS API richieste. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'EC2istanza e renderlo disponibile per le 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 Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAMutente.

Per sapere se utilizzare IAM ruoli o IAM utenti, consulta Quando creare un IAM ruolo (anziché un utente) nella Guida per l'IAMutente.

Come funziona AWS Security Incident Response 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. IAMgli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (dispone delle autorizzazioni) a utilizzare le risorse AWS Security Incident Response. IAMè un AWS servizio che è possibile utilizzare senza costi aggiuntivi.

IAMfunzionalità che è possibile utilizzare con AWS Security Incident Response	
IAMcaratteristica	Allineamento del servizio
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì

IAMfunzionalità che è possibile utilizzare con AWS Security Incident Response	
Chiavi relative alle condizioni della politica	Sì (globale)
ACLs	No
ABAC(tag nelle politiche)	Sì
Credenziali temporanee	Sì
Sessioni di accesso diretto () FAS	Sì
Ruoli di servizio	No
Ruoli collegati ai servizi	Sì

Indice

- Politiche basate sull'identità per la risposta agli incidenti di sicurezza AWS

Politiche basate sull'identità per la risposta agli incidenti di sicurezza AWS

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Con le policy IAM IAM basate su identità, puoi specificare operazioni e risorse consentite o rifiutate, nonché le condizioni in base alle quali le operazioni sono consentite o rifiutate. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per maggiori informazioni su tutti gli elementi che è possibile utilizzare in una JSON policy, consulta il riferimento agli elementi delle IAM JSON policy nella Guida per l'IAMutente.

Indice

- Esempi di policy basate su identità
- Best practice per le policy
- Utilizzo della console AWS Security Incident Response

- Consentire agli utenti di visualizzare le loro autorizzazioni
- Chiavi delle condizioni della policy per AWS Security Incident Response
- Accedi agli elenchi di controllo (ACLs) in AWS Security Incident Response

Esempi di policy basate su identità

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare le 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 API. Un IAM amministratore può creare IAM politiche per concedere agli utenti il permesso di eseguire azioni sulle risorse di cui hanno bisogno. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una politica IAM basata sull'identità utilizzando questi documenti di esempioJSON, consulta Creazione di IAM politiche nella Guida per l'IAMutente.

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, vedere Azioni, risorse e chiavi di condizione per 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 le risorse di AWS Security Incident Response nel tuo account. Queste azioni possono comportare costi per il tuo account. AWS Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo account. AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta le politiche AWS gestite o le politiche AWS gestite per le funzioni lavorative nella Guida per l'IAMutente.

Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie 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 privilegi minimi. Per ulteriori informazioni sull'utilizzo per applicare le autorizzazioni, consulta Politiche e autorizzazioni nella Guida IAM per l'utente. IAM IAM

Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzandoSSL. È inoltre possibile utilizzare condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite un AWS servizio specifico, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta Elementi IAM JSON della politica: Condizione nella Guida IAM per l'utente.

Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy () e alle best practice. JSON IAM IAM Access Analyzer fornisce più di 100 controlli delle policy e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, vedere Convalida delle policy di IAM Access Analyzer nella Guida per l'utente. IAM

Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede l'utilizzo di IAM utenti o un utente root nel tuo AWS account, attiva questa opzione MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, vedere Configurazione dell'APIaccesso MFA protetto nella Guida per l'IAMutente.

Per ulteriori informazioni sulle procedure consigliate inIAM, consulta la sezione Procedure consigliate in materia di sicurezza IAM nella Guida per l'IAMutente.

Utilizzo della console AWS Security Incident Response

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 risorse AWS Security Incident Response presenti nel 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 autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso il AWS CLI. AWS API Consenti invece l'accesso solo alle azioni che corrispondono all'APIoperazione che stanno cercando di eseguire.

Allega il AWS Security Incident Response Access o la policy ReadOnly AWS gestita per garantire che utenti e ruoli possano utilizzare la console di servizio. Per ulteriori informazioni, consulta Aggiungere autorizzazioni a un utente nella Guida per l'IAMutente.

Consentire agli utenti di visualizzare le loro autorizzazioni

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

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "ViewOwnUserInfo",
"Effect": "Allow",
"Action": [
"iam:GetUserPolicy",
"iam:ListGroupsForUser",
"iam:ListAttachedUserPolicies",
"iam:ListUserPolicies",
"iam:GetUser"
],
"Resource": ["arn:AWS:iam::*:user/${AWS:username}"]
},
{
"Sid": "NavigateInConsole",
"Effect": "Allow",
"Action": [
"iam:GetGroupPolicy",
"iam:GetPolicyVersion",
"iam:GetPolicy",
"iam:ListAttachedGroupPolicies",
"iam:ListGroupPolicies",
"iam:ListPolicyVersions",
"iam:ListPolicies",
"iam:ListUsers"
],
"Resource": "*"
}
]
}
```

Politiche basate sulle risorse all'interno di Security Incident Response AWS

Supporta le policy basate su risorse: no

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

Per ulteriori informazioni, consulta la sezione Cross Account Resource Access nella IAM Guida per l'utente. IAM

Azioni politiche per la risposta agli incidenti AWS di sicurezza

Azioni politiche di supporto: Sì

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

L'elemento Azione di una JSON policy 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' AWS APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

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

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

Le azioni politiche in AWS Security Incident Response 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"," Security Incident Response -identity:action2"]AWS

Risorse politiche per Amazon AWS Security Incident Response

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

L'elemento della JSON policy Resource specifica l'oggetto o gli oggetti a cui si applica l'azione. Le dichiarazioni devono includere una risorsa o un NotResource elemento. Come best practice, specifica una risorsa utilizzando il relativo Amazon Resource Name (ARN). È possibile eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

"Resource": "*"

Chiavi delle condizioni della policy per AWS Security Incident Response

Supporta le chiavi delle condizioni delle policy specifiche del servizio: No

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale 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'ANDoperazione 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, puoi concedere a un utente IAM l'autorizzazione per accedere a una risorsa solo se è stata taggata con il nome utente IAM. Per ulteriori informazioni, consultate Elementi IAM della politica: variabili e tag nella Guida per l'IAMutente.

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'IAMutente.

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

SupportiACLs: 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. ACLssono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

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

Supporti ABAC (tag nelle politiche): Sì

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo passo diABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere. ABACè utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

Per controllare l'accesso in base ai tag, si forniscono 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 è Sì per il servizio. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorse, il valore è Partial. Per ulteriori informazioni suABAC, vedi Cos'èABAC? nella Guida IAM per l'utente. Per visualizzare un tutorial con i passaggi per la configurazioneABAC, consulta Utilizzare il controllo di accesso basato sugli attributi (ABAC) nella Guida per l'IAMutente.

Credenziali temporanee con Amazon AWS Security Incident Response

Supporta le credenziali temporanee: sì

AWS i servizi non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi AWS i servizi che funzionano con credenziali temporanee, consulta AWS i servizi che funzionano con IAM nella Guida per l'IAMutente. Stai utilizzando credenziali temporanee se accedi alla Console di AWS gestione utilizzando qualsiasi metodo tranne il nome utente e la 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 sul cambio di ruolo, consulta Passare a un ruolo (console) nella Guida per l'IAMutente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI o AWS API. È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, vedere Credenziali di sicurezza temporanee in. IAM

Sessioni di accesso diretto per AWS Security Incident Response

Supporta sessioni di accesso inoltrato (FAS): Sì

Quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che quindi avvia un'altra azione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama un AWS servizio, in combinazione con il servizio richiedente per effettuare richieste ai AWS servizi a valle. FASle richieste 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 FAS delle politiche relative alle richieste, consulta Forward access sessions.

Risoluzione dei problemi AWS di identità e accesso a Security Incident Response

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

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 risorse di AWS Security Incident Response

Non sono autorizzato a eseguire alcuna azione

Se ricevi un errore che indica che non disponi dell'autorizzazione per eseguire un'operazione, le tue policy devono essere aggiornate in modo che ti sei consentito eseguire tale operazione.

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

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

In questo caso, la politica per l'utente mateojackson deve essere aggiornata per consentire l'accesso alla risorsa utilizzando l'azione Security Incident Response:. my-example-widget AWS 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'PassRole azione iam:, le tue policy devono essere aggiornate per consentirti di trasferire 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 IAM utente 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 passare 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 risorse di AWS Security Incident Response

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 ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon AWS Security Incident Response supporta queste funzionalità, consulta Come funziona AWS Security Incident ResponseIAM.
- Per sapere come fornire l'accesso alle tue risorse su più AWS account di tua proprietà, consulta Fornire l'accesso a un IAM utente in un altro AWS account di tua proprietà nella Guida per l'IAMutente.

- Per informazioni su come fornire l'accesso alle tue risorse ad AWS account di terze parti, consulta Fornire l'accesso agli AWS account di proprietà di terzi nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso agli utenti autenticati esternamente (federazione delle identità) nella Guida per l'IAMutente.
- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse tra account nella Guida per l'utente. IAM IAM

Utilizzo dei ruoli di servizio

Supporta i ruoli di servizio: No

Un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio da IAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un AWS servizio nella Guida per l'IAMutente.

Uso di ruoli collegati ai servizi

Ruoli collegati ai servizi per Security Incident Response AWS

Indice

- AWS SLR: AWSServiceRoleForSecurityIncidentResponse
- AWS SLR: AWSServiceRoleForSecurityIncidentResponse_Triage
- Regioni supportate per i ruoli collegati al servizio AWS Security Incident Response

Supporta 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'azione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare, ma non modificare le autorizzazioni dei ruoli collegati ai servizi.

Un ruolo collegato al servizio semplifica la configurazione AWS di Security Incident Response perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS Security Incident

Response definisce le autorizzazioni dei suoi ruoli collegati al servizio e, se non diversamente definito, solo AWS Security Incident Response può assumerne i ruoli. Le autorizzazioni definite includono la policy di trust 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 ai servizi per tale servizio.

AWS SLR: AWSServiceRoleForSecurityIncidentResponse

AWS Security Incident Response utilizza il ruolo collegato al servizio (SLR) denominato AWSServiceRoleForSecurityIncidentResponse AWS Security Incident Response policy per identificare gli account sottoscritti, creare casi e etichettare le risorse correlate.

Autorizzazioni

Il ruolo AWSServiceRoleForSecurityIncidentResponse collegato al servizio prevede che il ruolo venga assunto dal seguente servizio:

- `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.
- TagResource: consente di configurare le risorse dei tag di servizio come parte del servizio.

Gestione del ruolo

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando ti iscrivi a AWS Security Incident Response nel AWS Management Console, il AWS CLI, o il AWS API, il servizio crea per te 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 ai servizi, 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 (ad esempio un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi, devi configurare le 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 il ruolo collegato al servizio (SLR) denominato AWSServiceRoleForSecurityIncidentResponse_Triage AWS Security Incident Response policy 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.

Autorizzazioni

Il ruolo AWSServiceRoleForSecurityIncidentResponse_Triage 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 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 e raccogliere informazioni per indagare su potenziali incidenti. Questa azione viene eseguita su qualsiasi AWS risorsa.
- AWS Security Hub: consente al servizio di ottimizzare i servizi di sicurezza per ridurre il rumore generato dagli avvisi e raccogliere informazioni per indagare su potenziali incidenti. Questa azione viene eseguita su qualsiasi AWS risorsa.

Gestione del ruolo

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando ti iscrivi a AWS Security Incident Response nel AWS Management Console, il AWS CLI, o il AWS API, il servizio crea per te il ruolo collegato al servizio.

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando entri a far parte del servizio, il ruolo collegato al servizio viene nuovamente creato per te.

Per consentire a un'entità IAM (ad esempio un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi, devi configurare le autorizzazioni. Per ulteriori informazioni, consulta le autorizzazioni dei ruoli collegati al servizio nella Guida per l'utente. IAM

Regioni supportate per i ruoli collegati al servizio 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)
- US West (Oregon)
- Stati Uniti orientali (Virginia)
- UE (Francoforte)
- UE (Irlanda)
- UE (Londra)
- UE (Stoccolma)
- Asia Pacifico (Singapore)
- Asia Pacifico (Seoul)

- Asia Pacifico (Sydney)
- Asia Pacifico (Tokyo)
- Canada (Centrale)

AWS Policy gestite

Una policy AWS gestita è una policy 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 IAMche forniscono al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste politiche coprono casi d'uso comuni e sono disponibili nel tuo AWS account. Per ulteriori informazioni sulle politiche AWS gestite, consulta le politiche AWS gestite nella Guida IAM per l'utente.

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 un elenco e le descrizioni delle politiche relative alle funzioni lavorative, consulta le politiche AWS gestite per le funzioni lavorative nella Guida per l'utente. IAM

Indice

- AWS politica gestita: AWSSecurityIncidentResponseServiceRolePolicy
- AWS politica gestita: AWSSecurityIncidentResponseFullAccess
- AWS politica gestita: AWSSecurityIncidentResponseReadOnlyAccess

- AWS politica gestita: AWSSecurityIncidentResponseCaseFullAccess
- AWS politica gestita: AWSSecurityIncidentResponseTriageServiceRolePolicy
- AWS Security Incident Response: aggiornamenti SLRs e policy gestite.

AWS politica gestita: AWSSecurityIncidentResponseServiceRolePolicy

AWS Security Incident Response utilizza la policy AWSSecurityIncidentResponseServiceRolePolicy AWS gestita. Questa policy AWS gestita è associata al ruolo AWSServiceRoleForSecurityIncidentResponsecollegato al servizio. La policy fornisce l'accesso a AWS Security Incident Response per identificare gli account sottoscritti, creare casi e taggare le risorse correlate.

> **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.
- TagResource: consente di configurare le risorse dei tag di servizio come parte del servizio.

È possibile visualizzare le autorizzazioni associate a questa politica nelle politiche AWS gestite per AWSSecurityIncidentResponseServiceRolePolicy.

AWS politica gestita: AWSSecurityIncidentResponseFullAccess

AWS Security Incident Response utilizza la policy AWSSecurityIncidentResponseAdmin AWS gestita. Questa politica garantisce l'accesso completo alle risorse del servizio e l'accesso alle risorse correlate Servizi AWS. Puoi utilizzare questa politica con i tuoi IAM responsabili 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:

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

È possibile visualizzare le autorizzazioni associate a questa politica nelle politiche AWS gestite per. AWSSecurityIncidentResponseFullAccess

AWS politica gestita: AWSSecurityIncidentResponseReadOnlyAccess

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

> **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:

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

È possibile visualizzare le autorizzazioni associate a questa politica nelle politiche gestite per. AWS AWSSecurityIncidentResponseReadOnlyAccess

AWS politica gestita: AWSSecurityIncidentResponseCaseFullAccess

AWS Security Incident Response utilizza la policy AWSSecurityIncidentResponseCaseFullAccess AWS gestita. La policy garantisce l'accesso completo alle risorse relative ai casi di assistenza. Puoi utilizzare questa politica con i tuoi IAM responsabili 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:

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

È possibile visualizzare le autorizzazioni associate a questa politica nelle politiche AWS gestite per. AWSSecurityIncidentResponseCaseFullAccess

AWS politica gestita: AWSSecurityIncidentResponseTriageServiceRolePolicy

AWS Security Incident Response utilizza la policy AWSSecurityIncidentResponseTriageServiceRolePolicy AWS gestita. Questa policy AWS gestita è associata al ruolo collegato al servizio AWSServiceRoleForSecurityIncidentResponse_Triage.

La policy fornisce l'accesso a AWS Security Incident Response 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. Non puoi collegare 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`triage.security-ir.amazonaws.com`.
- Amazon GuardDuty: consente al servizio di ottimizzare i servizi di sicurezza per ridurre il rumore degli avvisi e raccogliere informazioni per indagare su potenziali incidenti. Questa azione viene eseguita su qualsiasi AWS risorsa.
- AWS Security Hub: consente al servizio di ottimizzare i servizi di sicurezza per ridurre il rumore generato dagli avvisi e raccogliere informazioni per indagare su potenziali incidenti. Questa azione viene eseguita su qualsiasi AWS risorsa.

È possibile visualizzare le autorizzazioni associate a questa politica nelle politiche AWS gestite per AWSSecurityIncidentResponseTriageServiceRolePolicy.

AWS Security Incident Response: aggiornamenti SLRs e policy gestite.

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

Modifica	Descrizione	Data
NuovoSLR: AWSServiceRoleForS	Nuovo ruolo collegato al servizio e policy allegata che consentono l'accesso del servizio AWS Organizations agli account per identificare l'appartenenza.	1 dicembre 2024

Modifica	Descrizione	Data
ecurityIn cidentResponse Nuova politica gestita: AWSSecuri tyInciden tResponse ServiceRo lePolicy.		
NuovoSLR: AWSServic eRoleForS ecurityIn cidentRes ponse_Triage Nuova politica gestita: AWSSecuri tyInciden tResponse TriageSer viceRolePolicy	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.	1 dicembre 2024
Nuova politica gestita: AWSSecuri tyInciden tResponse FullAccess	AWS Security Incident Response ne aggiunge una nuova da SLR allegare IAM ai principali per le azioni di lettura e scrittura del servizio.	1 dicembre 2024

Modifica	Descrizione	Data
Nuovo ruolo di policy gestita: AWSSecurityIncidentResponseReadOnlyAccess	AWS Security Incident Response ne aggiunge uno nuovo SLR da allegare ai IAM principali per le azioni di lettura	1 dicembre 2024
Nuovo ruolo di policy gestita: AWSSecurityIncidentResponseCaseFullAccess	AWS Security Incident Response ne aggiunge uno nuovo SLR da allegare ai IAM principali per le azioni di lettura e scrittura per i casi di assistenza.	1 dicembre 2024
Ha iniziato a tenere traccia delle modifiche.	Ha iniziato a tenere traccia delle modifiche per AWS Security Incident Response SLRs e per le policy gestite	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 base di sicurezza che soddisfi gli obiettivi delle applicazioni eseguite nel cloud, sei in grado di rilevare deviazioni a cui puoi 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 PCIRAMP, Fed HIPAA e altri.

AWS Security Incident Response non è stata valutata la conformità ai suddetti programmi.

Per un elenco dei AWS servizi che rientrano nell'ambito di specifici programmi di conformità, vedere 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 normative applicabili.AWS 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 HIPAA sicurezza e la conformità: questo white paper descrive in che modo le aziende possono utilizzare per creare applicazioni conformi. AWS HIPAA
- AWS risorse per la conformità: una raccolta di cartelle di lavoro e guide applicabili in base al settore e/o all'ubicazione.
- 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, ad esempio 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 una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di AWS Security Incident Response e delle altre AWS soluzioni. AWS Security Incident Response attualmente supporta i seguenti AWS servizi per monitorare l'organizzazione e le attività che si svolgono al suo interno.

AWS CloudTrail — Con CloudTrail è possibile acquisire API le chiamate 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'utilizzo del AWS Security Incident Response oppure puoi 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 ai Termini di AWS servizio, il team addetto ai soccorritori di AWS Security Incident Response avrà accesso alla cronologia DNS e ai dati di CloudTrail VPC registro di S3. Questi dati possono essere utilizzati durante incidenti di sicurezza attivi quando viene aperta una segnalazione nel portale del servizio AWS Security Incident Response.

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

- Transport Layer Security (TLS). Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Suite di crittografia con perfetta segretezza di inoltro (PFS) come (Ephemeral Diffie-Hellman) o DHE (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 che è associata a un'entità IAM. Oppure puoi utilizzare il Security Token Service () per generare credenziali di sicurezza temporanee per firmare le richieste.AWSAWS STS

Analisi della configurazione e delle vulnerabilità

Sei responsabile della gestione dei ruoli di contenimento del servizio e dei set di AWS 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 confuso problema secondario consiste nell'utilizzare l'esatto Amazon Resource Name (ARN) della risorsa che desideri consentire. Se non conosci l'intera ARN risorsa o se stai specificando più risorse, usa la chiave AWS: SourceArn global context condition con caratteri jolly (*) per le parti sconosciute di. 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 (Quote di Servizio)

AWS Risposta agli incidenti di sicurezza

Le tabelle seguenti elencano le quote per le risorse AWS Security Incident Response per il tuo AWS-account;. Alcune quote possono essere aumentate oltre quelle indicate di seguito con l'approvazione del responsabile del servizio. Salvo diversa indicazione, le quote sono calcolate per regione.

	Nome	Predefinita	Adattabile	Commenti
1	Casi attivi AWS supportati	10	Sì (fino a 50)	Il numero di casi attivi a cui è richiesta assistenza. AWS CIRT
2	Casi attivi autogestiti	50	Sì (fino a 100)	Il numero di casi attivi che utilizzano la piattaforma senza l'assistenza di AWS CIRT.
3	Casi supportati dal servizio creati entro 24 ore	10	No	Il numero di casi creati per la richiesta di assistenza è AWS CIRT stato creato in una finestra variabile di 24 ore.
4	Numero massimo di entità nel team di risposta	10	No	Il numero massimo di entità nel team di risposta

	Nome	Predefinita	Adattabile	Commenti
	agli incidenti predefinito			agli incidenti predefinito.
5	Numero massimo di membri aggiuntivi per caso	30	No	Il numero massimo di entità associate a un caso. Inizialmente verrà compilato con le entità del team di risposta agli incidenti predefinito.
6	Numero massimo di allegati del caso	50	Sì (fino a 100)	Il numero massimo di file che è possibile allegare a una custodia.
7	Dimensione massima dei commenti del caso	1000	No	Il numero massimo di caratteri in un commento al caso.
8	Dimensione massima del nome del file Case Allegation	255	No	Il numero massimo di caratteri in un nome di file.

AWS Guida tecnica sulla risposta agli incidenti di sicurezza

Indice

- Sintesi
- Sei tu Well-Architected?
- Introduzione
- Preparazione
- Operazioni
- Attività post-incidente
- Conclusioni
- Collaboratori
- Appendice A: Definizioni delle funzionalità cloud
- Appendice B: risorse per la risposta AWS 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 tu 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

AWS CAFFornisce linee guida a supporto del coordinamento tra le diverse parti delle organizzazioni che passano al cloud. La AWS CAF guida è suddivisa in diverse aree di interesse, denominate prospettive, che sono rilevanti per la creazione di sistemi IT basati sul cloud. La prospettiva sulla 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 r2, creata dal National Institute of Standards and Technology (). NIST Leggere e comprendere i concetti introdotti da è un utile prerequisito. NIST I concetti e le migliori pratiche di questa NIST guida verranno applicati alle AWS tecnologie in questo paper. Tuttavia, gli scenari di incidenti locali 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, così come i principi fondamentali di progettazione della risposta agli AWS incidenti, sono descritti in dettaglio in questa sezione.

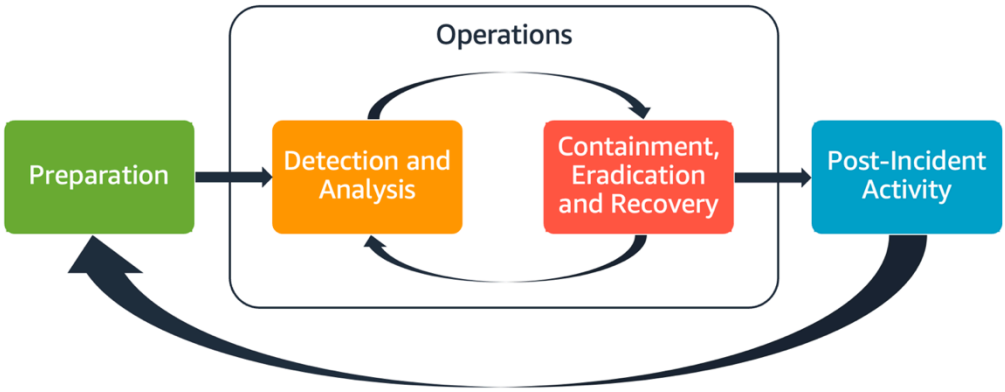
Aspetti della risposta AWS agli incidenti

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 NIST di risposta agli incidenti: 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 NIST incidenti 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 NISTSP 800-61 Computer Security Incident Handling Guide 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 ridistribuzione: se un'anomalia di sicurezza può essere attribuita a una configurazione errata, la correzione potrebbe essere semplice: basta rimuovere la varianza ridistribuendo le risorse con la configurazione corretta. Se viene identificato un possibile compromesso, verificate che la ridistribuzione 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 si risponde esclusivamente con AWS API meccanismi o in cui le cause principali sono associate alla configurazione o alle autorizzazioni relative alle risorse e la relativa registrazione orientata ai servizi.
- Dominio dell'infrastruttura: gli incidenti nel dominio dell'infrastruttura includono attività relative ai dati o alla rete, come processi e dati sulle istanze Amazon Elastic Compute Cloud (EC2Amazon), il traffico verso le istanze EC2 Amazon 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 coinvolgere anche dei meccanismi. AWS API Nel dominio dell'infrastruttura, puoi utilizzare una combinazione di AWS APIs strumenti digitali forensics/incident response (DFIR) all'interno di un sistema operativo guest, ad esempio un'EC2istanza Amazon 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 (AmazonEBS) 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 delle informazioni di sicurezza e della gestione degli eventi (). 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.

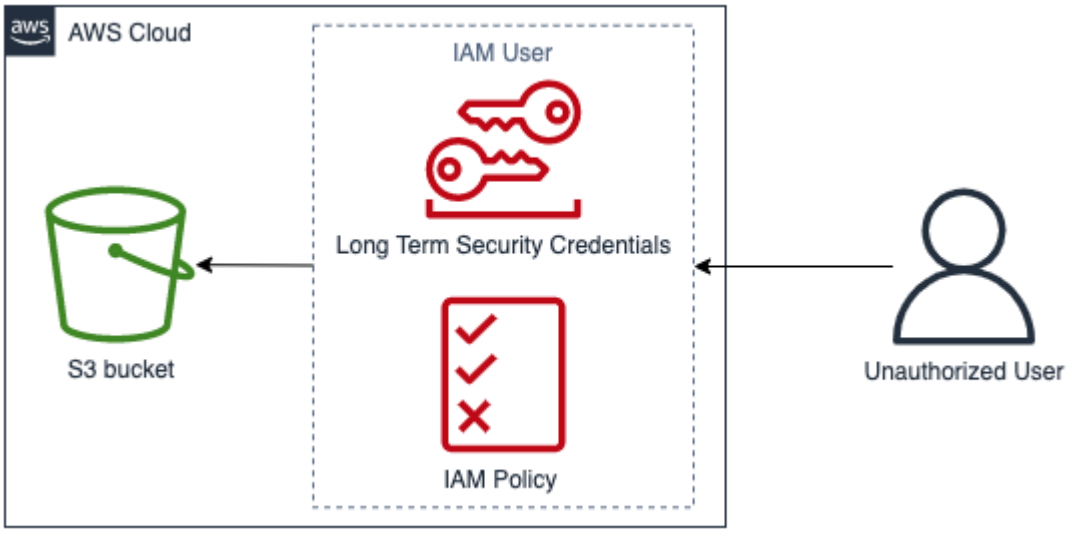
È estremamente importante creare e testare un piano di risposta agli incidenti appropriato e playbook appropriati che corrispondano al modello operativo in uso.

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, le IAM autorizzazioni, i metadati delle risorse, la fatturazione e altre aree del cliente. Questo dominio è diverso per 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 API le chiamate, anziché la tradizionale risposta basata sull'host e sulla rete. Nel dominio del servizio, non interagirai 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 architettonico. In questo caso, un utente non autorizzato ottiene le credenziali di sicurezza a lungo termine di un utente. IAM L'IAMutente dispone di una IAM policy 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 CloudTraildi 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 endpoint pubblici e privati disponibili in molte aree geografiche in tutto il mondo. RESTful API I clienti possono accedervi APIs 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 IAM principale all'interno di un account. AWS È possibile accedere a questi API endpoint 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.

A causa della natura API basata su AWS, un'importante fonte di log per rispondere agli eventi di sicurezza è quella AWS CloudTrail che tiene traccia delle API chiamate 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 Configper 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 API chiamate. 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 responsabile, affidabile, consultata e informata (RACI) 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, coinvolgere i proprietari/sviluppatori delle applicazioni e delle risorse interessate è fondamentale perché si tratta di esperti in materia (SMEs) in grado di fornire informazioni e contesto per contribuire alla misurazione dell'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 oSMEs, 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 in modo adeguato 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, dovreste 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 comprendere AWS le basi IAM AWS Organizations, i servizi di AWS registrazione e monitoraggio e i servizi di sicurezza. AWS

AWS offre workshop sulla sicurezza online (fare riferimento ai workshop AWS sulla sicurezza) 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.

Comprendi il tuo AWS ambiente

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

Support

Supportoffre 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 AWS Management Console (è richiesto l'accesso) come punto di contatto centrale per ricevere assistenza per problemi che riguardano AWS le tue risorse. L'accesso a Support è controllato daIAM. Per ulteriori informazioni su come accedere alle funzionalità di AWS Support, consulta Guida introduttiva Support.

Inoltre, se devi segnalare un abuso, contatta il team di AWS Trust and Safety.

AWS Team di risposta agli incidenti con i clienti () CIRT

Il AWS Customer Incident Response Team (CIRT) è 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.

Se ti AWS CIRT supporta, riceverai assistenza per il triage 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 contattarli AWS CIRT 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 Support piani Developer:
  1. Account e fatturazione
  2. Servizio: Account
  3. Categoria: Sicurezza
  4. Severità: domanda importante

- Clienti con Support piani aziendali:
  1. Account e fatturazione
  2. Servizio: Account
  3. Categoria: Sicurezza
  4. Severità: domanda urgente che ha un impatto sull'attività

- Clienti con Support piani Enterprise:
  1. Account e fatturazione
  2. Servizio: Account
  3. Categoria: Sicurezza
  4. Severità: domanda critica sul rischio aziendale

- Clienti con abbonamenti AWS Security Incident Response: aprire la console Security Incident Response all'indirizzo https://console.aws.amazon.com/security-ir/

DDoSsupporto di risposta

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. Support DDoS 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) fornisce una gestione continua dell' AWS infrastruttura in modo da potersi concentrare sulle applicazioni. Implementando le migliori pratiche per la manutenzione dell'infrastruttura, AMS contribuisce a ridurre i costi operativi e i rischi. AMSautomatizza attività comuni come richieste di modifica, monitoraggio, gestione delle patch, sicurezza e servizi di backup e fornisce servizi per l'intero ciclo di vita per la fornitura, l'esecuzione e il supporto dell'infrastruttura.

AMSsi assume la responsabilità dell'implementazione di una suite di controlli di sicurezza e fornisce una prima linea di risposta quotidiana agli avvisi. Quando viene avviato un avviso, AMS segue una serie standard di playbook automatici e manuali per verificare una risposta coerente. Questi playbook vengono condivisi con AMS i clienti durante l'onboarding in modo che possano sviluppare e coordinare una risposta. 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 IAM ruoli o utenti (o entrambi)? La tua autenticazione è AWS connessa a un provider di identità (IdP)?
  - Come si associa un IAM ruolo o un utente 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 IAM politiche 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 biglietteriaSIEM)?
  - 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?
  - Che cos'è DDoS il filtro esterno?

La documentazione dei diagrammi e dei processi tecnici interni semplifica 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 di 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, in un luogo 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 addetto ai 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 Squadra Rossa 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 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. AARDovrebbero misurare l'efficacia della simulazione e la risposta del team all'evento simulato in modo da poter monitorare i progressi nel tempo con simulazioni future.

Tecnologia

Se sviluppate e implementate le tecnologie appropriate prima che si verifichi un incidente di sicurezza, il personale addetto alla risposta agli incidenti sarà in grado di indagare, comprenderne l'ambito e intervenire tempestivamente.

Sviluppa la struttura AWS degli account

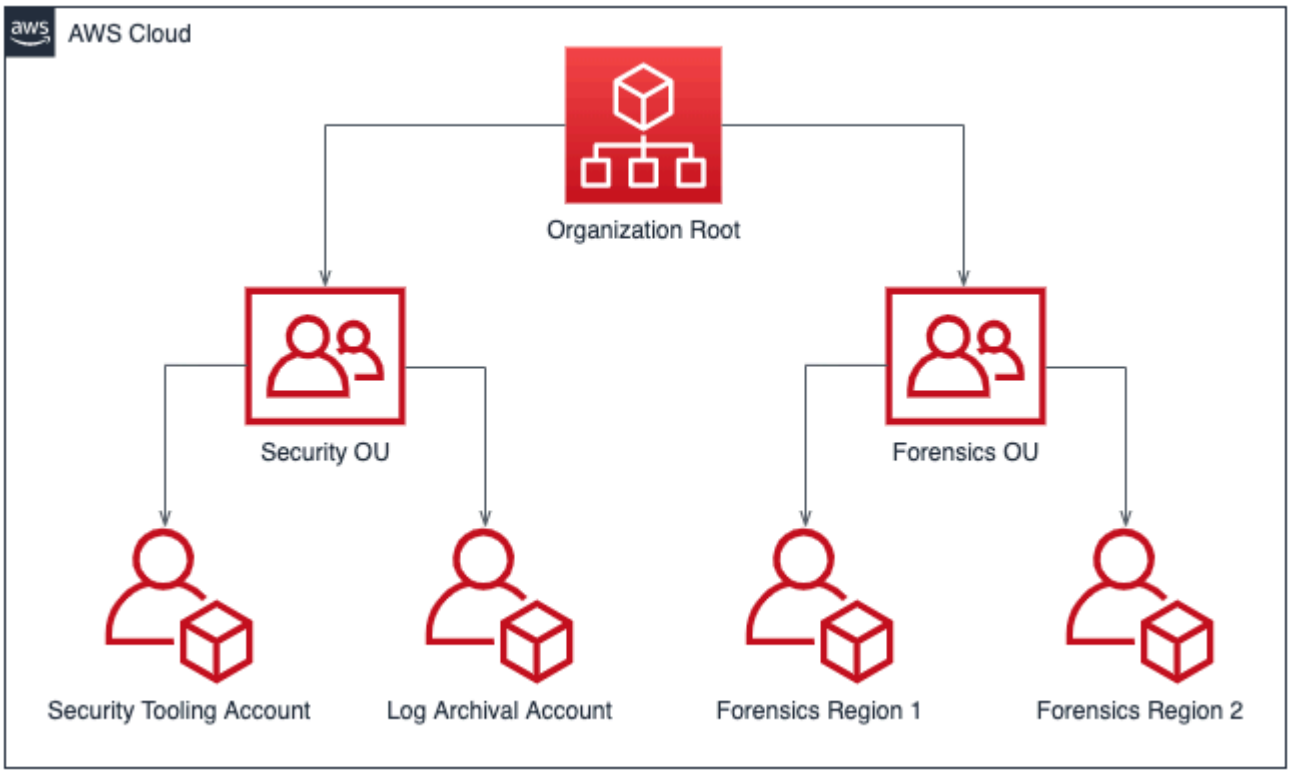
AWS Organizationsaiuta a gestire e governare centralmente un AWS ambiente man mano che si aumentano e si scalano AWS le risorse. Un' AWS organizzazione consolida AWS gli account in modo da poterli amministrare come un'unica unità. È possibile utilizzare le unità organizzative (OUs) per raggruppare gli 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

Sviluppa 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 evitare la reimpostazione della password dell'account root e la 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 an 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. È possibile 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 DNS firewall e AWS WAF le regole, ricevono input dall' AWS Advanced Threat Intelligence Group. Alcuni GuardDuty risultati vengono mappati nel MITREATT&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 ulteriori 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 degli account. AWS

AWS CloudTrail è un servizio di registrazione che tiene traccia delle API chiamate effettuate rispetto all'attività del servizio di acquisizione AWS di un AWS account. È abilitato per impostazione predefinita con la conservazione per 90 giorni degli eventi di gestione che possono essere recuperati tramite CloudTrail la funzione Event History utilizzando AWS Management Console, il, o un. AWS CLI AWS SDK 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 conservi CloudTrail i log per un massimo di sette anni e fornisca una funzione di interrogazione basata su una base. SQL

AWS consiglia ai clienti di VPC abilitare il traffico di rete e DNS i log utilizzando, rispettivamente, i log delle query del resolver VPCFlow Logs e Amazon Route 53, trasmettendoli in streaming su un bucket Amazon S3 o un gruppo di log. CloudWatch Puoi creare un log di VPC flusso per unaVPC,

una sottorete o un'interfaccia di rete. Per quanto riguarda VPC Flow Logs, potete scegliere in modo selettivo come e dove abilitare Flow Logs per ridurre i costi.

AWS CloudTrail Logs, VPC Flow Logs e i log delle query del resolver Route 53 sono la tripletta 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) e log delle applicazioni e del sistema operativo delle istanze Amazon. EKS EC2 the section called “Appendice A: Definizioni delle funzionalità cloud”Fai riferimento a per l'elenco completo delle opzioni di registrazione e monitoraggio.

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 i 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 informazioni di sicurezza e gestione degli eventi (). SIEM

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 una terza parte SIEM per eseguire query sugli ultimi 90 giorni di dati e utilizzare Athena per eseguire query oltre i 90 giorni a causa del costo di acquisizione 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, 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 fornisce tali indicazioni. NIST

Analisi forense 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 i AWS log pertinenti, ad esempio i log di VPC flusso e i log a AWS CloudTrail livello di AWS Config host. 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. Sì 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 ulteriori 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 la precisione 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

Domain	Elemento di preparazione	Elementi d'azione
Persone	Definisci ruoli e responsabilità.	• Identifica gli stakeholder pertinenti alla risposta agli incidenti. • Sviluppa un grafico responsabile, responsab ile, informato e consultato (RACI) per un incidente.
Persone	Formare il personale addetto alla risposta agli incidenti su AWS.	• Formare le parti interessa te alla risposta agli incidenti sulle AWS basi. • Forma gli stakeholder addetti alla risposta agli incidenti sui servizi di AWS sicurezza e monitoraggio. • Addestra gli stakehold er addetti alla risposta agli incidenti sul tuo AWS ambiente e su come è progettato.
Persone	Comprendi le opzioni di AWS supporto.	• Comprendi le differenz e nell' AWS assistenza, nel Customer Incident Response Team (CIRT), nel team di DDoS risposta (DRT) eAMS. • Comprendi il percorso di triage e di escalation da seguire CIRT durante un evento di sicurezza attivo, se necessario.

Domain	Elemento di preparazione	Elementi d'azione
Processo	Sviluppa un piano di risposta agli incidenti.	• 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 piano di comunicazione, le definizioni degli incidenti e le fasi di risposta agli incidenti.
Processo	Documenta e centralizza i diagrammi di architettura.	• Documenta i dettagli sulla configurazione AWS dell'ambiente in base alla struttura degli account, agli utilizzi dei servizi, ai IAM modelli e ad altre funzional ità di base della configura zione. AWS • Sviluppa diagrammi di architettura delle tue architetture cloud.
Processo	Sviluppa dei playbook di risposta agli incidenti.	• 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

Domain	Elemento di preparazione	Elementi d'azione
Processo	Esegui simulazioni regolari.	• 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.	• 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 identific are la titolarità e il contesto dei risultati.	• Pianifica una strategia per l'etichettatura e i tag che desideri associare alle tue risorse. AWS • Implementa e applica la strategia di tagging.

Domain	Elemento di preparazione	Elementi d'azione
Tecnologia	Aggiorna le informazioni di contatto dell' AWS account.	• 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.	• Definisci l'accesso di cui avranno bisogno i soccorrit ori per rispondere a un incidente. • Implementa, testa e monitora l'accesso.
Tecnologia	Comprendi il panorama delle minacce.	• Sviluppa modelli di minaccia del tuo ambiente e delle tue applicazioni. • Integra e utilizza l'intelli gence sulle minacce informatiche.

Domain	Elemento di preparazione	Elementi d'azione
Tecnologia	Seleziona e configura i registri.	• 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.	• 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 all'incidente in base all'attività 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, Amazon AWS ConfigInspector, Access Analyzer e Network Access Analyzer generano risultati che possono essere utilizzati per creare avvisi. IAM
- 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 relativa alla creazione di un allarme di fatturazione per monitorare gli AWS addebiti stimati. A tal fine, è necessario monitorare tale evenienza.
- 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 aiutarvi a raggiungere i vostri obiettivi di sicurezza. Per la risposta agli incidenti, collabora con prodotti dotati di funzionalità di rilevamento e risposta degli endpoint (EDR) o SIEM possono aiutarti a supportare i tuoi obiettivi di risposta agli incidenti. Per ulteriori informazioni, vedere Security Partner Solutions e Security Solutions nel Marketplace AWS.
- AWS fiducia e sicurezza: Support 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 documentothe 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 di un' AWS organizzazione (). SCP Se si verifica un'attività dell'utente root oltre la linea di base prevista, un controllo investigativo implementato con una EventBridge regola e un SNS argomento avviserà il centro operativo di sicurezza ()SOC. Il controllo reattivo prevede la SOC selezione del playbook appropriato, l'esecuzione di analisi e il lavoro 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 ne determinerà la vera criticità. Ad esempio, un'organizzazione utilizza Amazon GuardDuty come componente del controllo investigativo utilizzato per EC2 le istanze che fanno parte di un carico di lavoro. Il risultato `Impact:EC2/SuspiciousDomainRequest.Reputation` viene generato e ti informa che l'EC2istanza Amazon elencata nel tuo carico di lavoro sta interrogando un nome di dominio sospettato di essere dannoso. Questo avviso è impostato per impostazione predefinita a bassa gravità e, man mano che la fase di analisi procede, è stato stabilito che diverse centinaia di EC2 istanze 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 di 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 API richiesta anomala nel tuo account». Se approfondisci la documentazione, ti viene detto che «Il modello ML valuta tutte le API richieste nell'account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari», a indicare che questo risultato è di natura comportamentale.
- Per la scopertaImpact:S3/MaliciousIPCaller, GuardDuty sta analizzando API le chiamate 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 che trova 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, puoi 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 usare 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, i risultati dell'analisi possono essere correlati all'obiettivo del punto di ripristino (RPO) e all'obiettivo del tempo di ripristino () del carico di lavoro correlato, adattandoli alla criticità degli avvisi, che avvieranno l'allocazione delle risorse e tutte le attività successive. RTO 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 agli indirizzi IP pubblici, ai nomi di dominio e agli hash dei 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 intelligence sulle minacce possono essere utilizzate nelle SQL query per correlare elementi di registro come indirizzi IP e nomi di dominio, fornendo una visualizzazione più approfondita 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 le AWS API attività eseguite dall'identità o dalla risorsa dell'organismo di allerta nel momento dell'avviso, fornendo informazioni aggiuntive tra cui `eventSource` `eventNameSourceIPAddress`, e `userAgent` sull'APIattività identificata. Eseguendo queste interrogazioni in modo automatizzato, gli addetti alle risposte possono risparmiare tempo durante il triage e disporre di un contesto aggiuntivo che consenta di 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 archiviare 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, inclusi log del piano di servizio/controllo (eventi dati Amazon CloudTrail S3, VPC Flow Logs), dati (metadati e oggetti Amazon S3) e risorse (database, istanze Amazon). EC2

I log del piano di servizio/controllo 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 una parte copy/snapshot of the system running the database, creating a copy/snapshot dell'intero database stesso oppure interrogando ed estraendo determinati dati e registri dal database pertinenti all'indagine.

Per EC2 le istanze di Amazon, 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'EC2istanza Amazon è il seguente:

1. Acquisisci metadati dell'istanza: acquisisci i metadati dell'istanza pertinenti all'indagine e alle query sui 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 EBS volumi collegati e applica i tag appropriati sia per la denotazione visiva che per l'uso nelle 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 (EBSistantanee): acquisisce un'EBSistantanea dei EBS volumi 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 raccolta di risposte e artefatti in tempo reale se utilizzi volumi di Instance Store.
4. Acquisizione di memoria: poiché le EBS istantanee acquisiscono solo dati che sono stati scritti sul EBS volume Amazon, 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 un'indagine e un'analisi complete dell'istanza), potresti prendere in considerazione la chiusura dell'istanza, la creazione AMI di un'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 il monitoraggio quasi continuo di l'istanza (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:

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. Hanno SOC stabilito che il RDS database Amazon appartenente al marketing e alle vendite era accessibile al pubblico il 20 febbraio 2022. Hanno SOC interrogato i log di RDS accesso e hanno stabilito che l'indirizzo IP 198.51.100.23 è stato utilizzato il 20 febbraio 2022 con le credenziali `mm03434` appartenenti a Major Mary, uno degli sviluppatori web. Hanno SOC interrogato VPC Flow Logs e hanno stabilito che circa 256 MB di dati provenivano dallo stesso indirizzo IP nella stessa data (timestamp 2022-02-20T 15:50 +00Z). L'intelligence open source sulle minacce SOC ha stabilito 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'utilizzo 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.

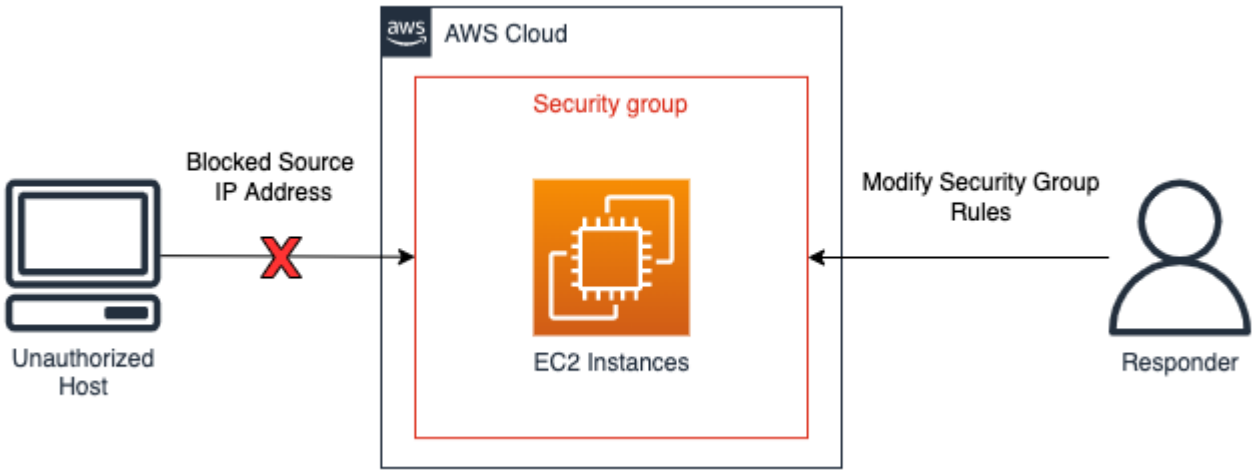
Contenimento della fonte

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 EC2 istanze Amazon o la rimozione di regole da un gruppo di sicurezza esistente può aiutare a contenere il traffico non autorizzato verso un'EC2istanza o AWS una risorsa Amazon. 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 (webACLs) 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 possibile vedere un esempio di contenimento dei sorgenti con un analista della risposta agli incidenti che modifica un gruppo di sicurezza di un'EC2istanza Amazon 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

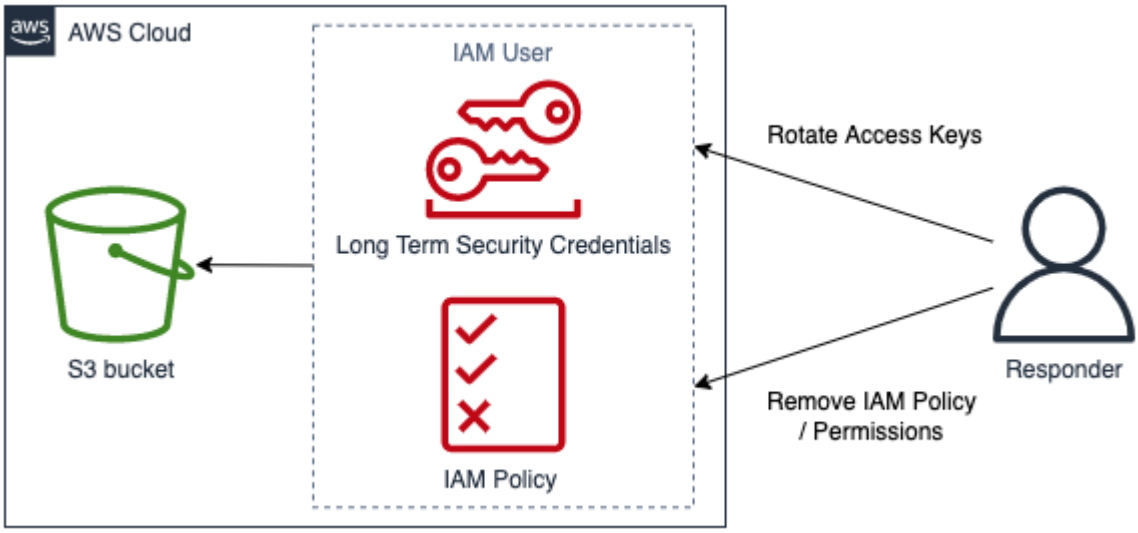
Tecnica e contenimento degli accessi

Impedisci l'uso non autorizzato di una risorsa limitando le funzioni e IAM i principali con accesso alla risorsa. Ciò include la limitazione delle autorizzazioni dei IAM responsabili che hanno accesso alla risorsa e include anche la revoca temporanea delle credenziali di sicurezza. Di seguito sono evidenziati esempi di tecniche e contenimento degli accessi utilizzando i servizi: AWS

- Limita le autorizzazioni: le autorizzazioni assegnate a un IAM principale 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 un IAM responsabile specifico. In questo caso, è possibile contenere l'accesso a una risorsa rimuovendo le autorizzazioni dal IAM principale da contenere. Questa operazione viene eseguita con il IAM servizio e può essere applicata utilizzando il AWS Management Console AWS CLI, il o un AWS SDK.
- Chiavi di revoca: le chiavi di IAM accesso vengono utilizzate dai IAM responsabili per accedere o gestire le risorse. Si tratta di credenziali statiche a lungo termine per firmare le richieste programmatiche indirizzate al sistema AWS CLI operativo AWS API e che iniziano con il prefisso AKIA(per ulteriori informazioni, consultate la sezione Informazioni sui prefissi degli ID univoci negli identificatori). IAM Per limitare l'accesso a un IAM principale in cui una chiave di IAM accesso 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 IAM principale 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 iniziare con il prefisso ASIA(per ulteriori informazioni, vedere la sezione Informazioni sui prefissi ID univoci negli identificatori). IAM Le credenziali temporanee vengono in genere utilizzate dai IAM ruoli 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 all'interno. IAM AWS Management ConsoleÈ inoltre possibile rilasciare credenziali di sicurezza temporanee agli IAM utenti (anziché ai IAM ruoli); tuttavia, al momento della stesura di questo documento, non è possibile revocare le credenziali di sicurezza temporanee per un IAM utente all'interno di. AWS Management Console Per gli eventi di sicurezza in cui la chiave di IAM accesso 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 all'IAMutente una policy in linea 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'IAMutente 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 il 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 illustrato nel diagramma seguente, con un operatore che risponde agli incidenti che ruota le chiavi di accesso o rimuove una IAM policy per impedire a un IAM utente di accedere a un bucket Amazon S3.



Esempio di tecnica e contenimento degli accessi

Contenimento della destinazione

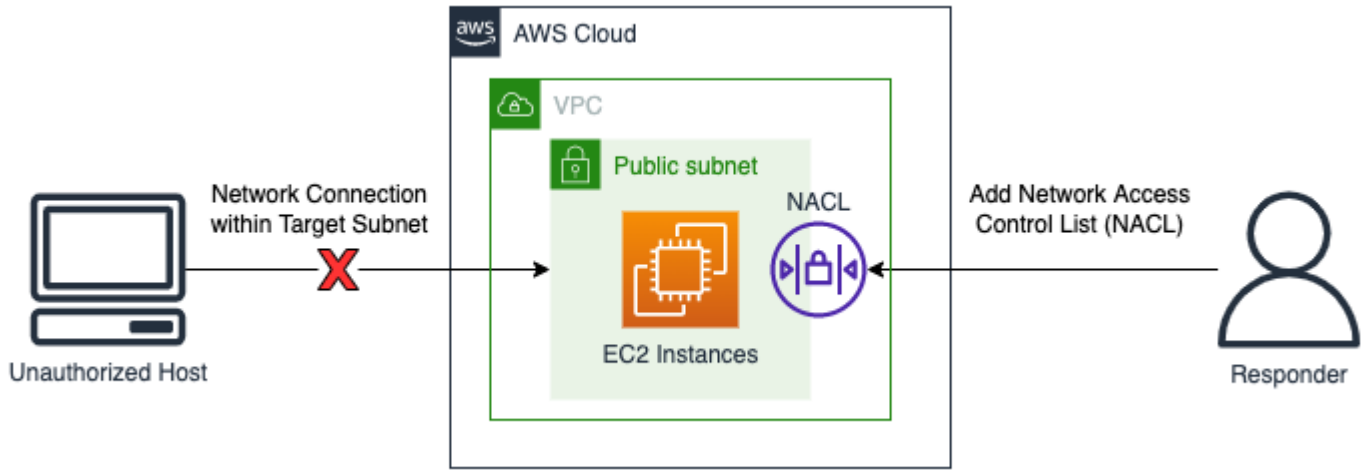
Il contenimento della destinazione è l'applicazione del filtraggio o del routing all'interno di un ambiente per impedire l'accesso a un host o a una risorsa mirati. In alcuni casi, il contenimento della destinazione implica anche una forma di resilienza per verificare che le risorse legittime vengano 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 (reteACLs) 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 (reteACL) influirà su tutte le risorse della sottorete, non solo sulle risorse a cui si accede senza autorizzazione. Le regole elencate all'interno di una rete ACL vengono elaborate in ordine dall'alto verso il basso, pertanto la prima regola di una rete esistente ACL deve essere configurata in modo da negare il traffico non autorizzato verso la risorsa e la sottorete di destinazione. In alternativa, è ACL possibile creare una rete completamente nuova con un'unica regola di negazione per il traffico in entrata e in uscita e associata alla sottorete contenente la risorsa di destinazione per impedire l'accesso alla sottorete utilizzando la nuova rete. ACL
- 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: l'isolamento VPCs può essere utilizzato per garantire un contenimento efficace delle risorse fornendo al contempo l'accesso al traffico legittimo (ad esempio antivirus (AV) o EDR soluzioni che richiedono l'accesso a Internet o a una console di gestione esterna). L'isolamento VPCs può essere preconfigurato prima di un evento di sicurezza per consentire indirizzi IP e porte validi e le risorse mirate possono essere immediatamente spostate in questo isolamento VPC 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 della risposta all'incidente. Un aspetto importante dell'utilizzo di un isolamento VPC è che le risorse, come EC2 le istanze, devono essere chiuse e riavviate nel nuovo isolamento prima dell'uso. VPC EC2Le istanze esistenti non possono essere spostate in un'altra o in un'altra zona di disponibilitàVPC. A tale scopo, segui i passaggi descritti in Come posso spostare la mia EC2 istanza Amazon in 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, e. AWS AWS Management Console AWS CLI AWS SDK

Nel diagramma seguente viene illustrato un esempio di contenimento della destinazione, con un analista della risposta agli incidenti che aggiunge una rete a una sottorete ACL 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 IAM identità del tuo account.
- Identifica accessi o modifiche non autorizzati al tuo account.
- Identifica la creazione di risorse o IAM utenti non autorizzati.
- Identifica sistemi o 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 l'applicazione aziendale e la sua eliminazione causerebbe dei tempi di inattività, è consigliabile recuperare la risorsa da backup sicuri verificati o riavviare il sistema da una posizione pulita AMI 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 potenzialmente non autorizzateIAM.
- 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'EC2istanza Amazon per motivi normativi, di conformità o legali, crea uno EBS snapshot Amazon 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 AmazonEBS, 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 ridistribuzione 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 IAM i responsabili che potrebbero essere state oggetto di abuso.

  - Se possibile, consigliamo di utilizzare i ruoli per i IAM dirigenti e la federazione 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, IAM i principali e l'esecuzione di una revisione di sicurezza dell'account per valutare il rischio residuo.

Conclusioni

Ogni fase operativa ha obiettivi, tecniche, metodologie e strategie unici. 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.	• Controlli di sicurezza per il rilevamento • 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.	• Convalida e analizza l'avviso • Registri delle interrogazioni • Informazioni sulle minacce • Automazione

Fase	Obiettivo	Tecniche e metodologie
Contenimento	Riduci al minimo e limita l'impatto dell'evento di sicurezza.	• Contenimento della fonte • Tecnica e contenimento degli accessi • Contenimento della destinazione
Eradicazione	Rimuovi risorse o artefatti non autorizzati correlati all'evento di sicurezza.	• 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.	• 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 verifichi che sia stato implementato?
- Qual è la tempistica entro cui verranno implementati e testati gli monitoring/preventative controls/process elementi aggiuntivi?

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 SOC momento in cui un membro 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 pipeline CI/CD 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

Parametro	Descrizione
Tempo medio di rilevamento	Tempo medio necessario per scoprire un possibile incidente di sicurezza

Parametro	Descrizione
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. IOCspossono esistere in una varietà di forme, tra cui indirizzi IP, domini, artefatti a livello di rete come TCP flag o payload, 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 precedenzaIOCs, 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. I test in base alle situazioni di sicurezza più recenti e critiche e alle funzionalità di risposta più importanti o più recenti e l'integrazione delle lezioni apprese nell'istruzione, nelle operazioni e nei processi/procedure verificheranno di essere in grado di migliorare continuamente i processi e il programma di risposta 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 ambiente. AWS 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. AWS Management Console 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 AWS API azioni:

- 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 a livello di oggetto di Amazon S3 (ad esempio `GetObject`, `DeleteObject`, e le operazioni `PutObject`API) e API 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 API le chiamate 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 EC2 istanze Amazon con un agente Logs. CloudWatch CloudWatch I log possono essere una destinazione per Route 53 DNS Queries AWS CloudTrail, VPC Flow Logs, funzioni Lambda e altre. 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. VPCs 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 VPC flusso 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 archiviarli 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 di analisi dei log SIEM e di terze parti.

Registri delle query di Route 53 Resolver: i log delle query di Route 53 Resolver consentono di registrare tutte le DNS query effettuate dalle risorse all'interno di Amazon Virtual Private Cloud (Amazon). VPC Che si tratti di un'EC2istanza Amazon, di una AWS Lambda funzione o di un contenitore, se risiede nel tuo Amazon VPC ed effettua una DNS query, questa funzionalità la registrerà; sarai quindi in grado di esplorare e comprendere meglio come funzionano le tue applicazioni.

Altri AWS registri: 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 Hub— AWS Security Hub offre ai clienti una visione completa degli avvisi di sicurezza ad alta priorità e degli stati di conformità tra gli account. AWS Security Hub aggrega, organizza e

dà priorità ai risultati di servizi AWS come Amazon, Amazon GuardDuty Inspector, 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 API chiamate insolite o implementazioni potenzialmente non autorizzate, indicando possibili compromissioni dell'account o delle risorse delle istanze AmazonEC2, 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 di AmazonEKS. La protezione di Amazon S3 consente di monitorare API le operazioni GuardDuty 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 sono 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 ConfigÈ 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 tenere traccia delle metriche, raccogliere e monitorare i file di registro, impostare allarmi e reagire automaticamente ai cambiamenti nelle tue AWS risorse. CloudWatch può monitorare AWS risorse, come EC2 istanze Amazon, tabelle Amazon DynamoDB e istanze RDS Amazon 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 Amazon Inspector o. API

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 e Amazon. EC2 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 S3 Glacier — Amazon S3 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 99,449%, offre una sicurezza completa ed è progettato per aiutarti a soddisfare i requisiti normativi. S3 Glacier offre query-in-place funzionalità che consentono di eseguire potenti analisi direttamente sui dati di archivio inattivi. Per mantenere bassi i costi e allo stesso tempo adattarsi alle diverse esigenze di recupero, S3 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 cercare 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 QuickSight, Amazon Machine Learning e Amazon. EMR

Appendice B: risorse per la risposta AWS 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
- Sviluppa i tuoi playbook di risposta agli incidenti: questo workshop è progettato per aiutarti a familiarizzare con lo sviluppo di playbook di risposta agli incidenti per. AWS
- Esempi di playbook sulla risposta agli incidenti: playbook che coprono gli scenari comuni affrontati dai clienti. AWS
- Creazione di un runbook di risposta agli AWS incidenti utilizzando i playbook Jupyter e CloudTrail Lake: questo workshop ti guida nella creazione di un playbook di risposta agli incidenti per il tuo ambiente utilizzando i notebook Jupyter e Lake. AWS CloudTrail

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 EC2 Amazon: questa guida all'implementazione fornisce una soluzione self-service per acquisire ed esaminare i dati EC2 dalle istanze e dai volumi allegati per l'analisi forense nel caso in cui venga rilevato un potenziale problema di sicurezza. Esiste un modello per implementare la soluzione. AWS CloudFormation
- 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.

Cronologia dei documenti

Modifica	Descrizione	Data
Aggiornato: aggiornamenti dai commenti dei clienti sui documenti.	Aggiornato https://docs.aws.amazon.com/security-ir/latest/userguide/setup: monitoring-and-investigation-workflows .html al modello stackset. Voci corrette da triage.security-ir.com a triage.security-ir.amazonaws.com È stata aggiunta una nota sulle connessioni tracciate per -Contain in .html. AWSSupport EC2Reversible https://docs.aws.amazon.com/security-ir/ latest/userguide/contain Risolto il problema del collegamento interrotto su - associated-accounts.html. https://docs.aws.amazon.com/security-ir/ latest/userguide/managing 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. È stata aggiunta una nota di chiarimento a https://docs.aws.amazon.com/en_us/	20 dicembre 2024

Modifica	Descrizione	Data
	security- ir/latest/userguid e/using - service-linked-rol es .html per AWS Organizat ions gli account di gestione.	

Modifica	Descrizione	Data
Aggiornato: aggiornamenti dei commenti dei clienti sui documenti.	Sono stati rimossi più duplicati AWS AWS nel testo. Collegamenti interrotti fissi su https://docs.aws.amazon.com /security-ir/ latest/userguide/ sir_tagging.html and https://d ocs.aws.amazon.com/security -ir/latest/userguide/service - name-info-in-cloudtrail .html. Aggiornamenti https://d ocs.aws.amazon.com/security -ir/ latest/userguide/contain a.html. È stato rimosso il > dal primo paragrafo . Sostituito AWSSuppor t -Contain EC2Revers ible con AWSSupport EC2Instance -Contain. Sostituito AWSSuppor t -C con -C. ontainIAM Reversible AWSSupport ontainIAMPrincipal Sostituit o AWSSupport -contains 3Reversible con -contains 3Resource. AWSSupport Formattazione aggiornat a sulla sicurezza https://d ocs.aws.amazon.com/en_us/ - .html ir/latest/userguide/ issues Quando si dice ai clienti di contattarci CIRT tramite un	10 dicembre 2024

Modifica	Descrizione	Data
	ticket di assistenza, https://docs.aws.amazon.com/security-ir/ latest/userguide/understand - response-teams-and-support .html ora offre opzioni da selezionare nei moduli di supporto. CloudWatch Eventi rimossi e sostituiti con EventBridge on https://docs.aws.amazon.com/security-ir/ latest/userguide/logging -and-events.html. Aggiornamenti grammaticali su https://docs.aws.amazon.com/security-ir/ latest/userguide/technique -access-containment.html. 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.	
Aggiornamento: politiche AWS gestite e ruoli collegati ai servizi.	Aggiornamenti alle politiche gestite e ai ruoli collegati ai servizi.	1 dicembre 2024
Avvio del servizio	Documenti di servizio iniziali per il lancio del servizio a re:Invent 2024	1 dicembre 2024

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.