Guida tecnica di AWS

# Guida sulla risposta agli incidenti di sicurezza di AWS

# Guida sulla risposta agli incidenti di sicurezza di AWS: Guida tecnica di AWS

# Table of Contents

# Guida sulla risposta agli incidenti di sicurezza di AWS

Data di pubblicazione: 23 novembre 2020 (Revisioni del documento)

Questa guida presenta una panoramica delle nozioni fondamentali per rispondere agli incidenti di sicurezza all'interno dell'ambiente AWS Cloud di un cliente. Si concentra su una panoramica della sicurezza del cloud e dei concetti di risposta agli incidenti e identifica le funzionalità, i servizi e i meccanismi cloud disponibili per i clienti che stanno rispondendo ai problemi di sicurezza.

Questo documento è destinato a coloro che ricoprono ruoli tecnici e presuppone che si abbia familiarità con i principi generali della sicurezza delle informazioni, una conoscenza di base della risposta agli incidenti negli attuali ambienti On-Premise e una certa familiarità con i servizi cloud.

# Introduzione

La sicurezza è la massima priorità per AWS. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete costruita per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza. AWS Cloud si avvale di un modello di responsabilità condivisa. AWS gestisce la sicurezza del cloud. La responsabilità per la sicurezza nel cloud spetta al cliente. Ciò significa che mantieni il controllo della sicurezza che scegli di implementare. Hai accesso a centinaia di strumenti e servizi che aiutano a raggiungere i tuoi obiettivi di sicurezza. Queste funzionalità aiutano a stabilire una base di sicurezza che soddisfi i tuoi obiettivi per le applicazioni in esecuzione nel cloud.

Quando si verifica una deviazione dalla linea di base (ad esempio a causa di un'errata configurazione), potrebbe essere necessario rispondere e indagare. Per farlo con successo, devi comprendere i concetti di base della risposta agli incidenti di sicurezza all'interno dell'ambiente AWS, nonché i problemi che devi considerare per preparare, istruire e formare i tuoi team del cloud prima che si verifichino problemi di sicurezza. È importante sapere quali controlli e funzionalità è possibile utilizzare, esaminare esempi attuali per risolvere potenziali problemi e identificare i metodi di correzione che è possibile utilizzare per sfruttare l'automazione e migliorare la velocità di risposta.

Poiché la risposta agli incidenti di sicurezza può essere un argomento complesso, ti invitiamo a iniziare in piccolo, sviluppare runbook, sfruttare le funzionalità di base e creare una libreria iniziale di meccanismi di risposta agli incidenti da cui eseguire iterazioni e migliorare. Questo lavoro iniziale dovrebbe includere il tuo ufficio legale e i team che non sono coinvolti nella sicurezza, in modo da poter comprendere meglio l'impatto che la risposta agli incidenti (IR) e le scelte che hai fatto hanno sui tuoi obiettivi aziendali.

Argomenti



# Prima di iniziare

Oltre a questo documento, ti invitiamo a esaminare le best practice per la sicurezza, l'identità e la conformità e il whitepaper Security Perspective of the AWS Cloud Adoption Framework (CAF)

(Prospettiva di sicurezza di AWS Cloud Adoption Framework (CAF)). AWS CAF fornisce linee guida che supportano il coordinamento tra le diverse parti delle organizzazioni che stanno passando al cloud. Le linee guida CAF sono suddivise in diverse aree di interesse che sono rilevanti per l'implementazione di sistemi IT basati sul cloud, che chiamiamo prospettive. La prospettiva di sicurezza descrive come implementare un programma di sicurezza in diversi flussi di lavoro, uno dei quali si concentra sulla risposta agli incidenti. Questo documento descrive alcune delle nostre esperienze nell'aiutare i clienti a valutare e implementare meccanismi di successo in quel flusso di lavoro.

# Prospettiva di sicurezza di AWS CAF

La prospettiva di sicurezza include quattro componenti:

- I controlli di direzione definiscono i modelli di governance, rischio e conformità in cui opera l'ambiente.
- I controlli di prevenzione proteggono i carichi di lavoro e riducono le minacce e le vulnerabilità.
- I controlli di rilevazione consentono di avere piena visibilità e trasparenza riguardo al funzionamento delle implementazioni in AWS.
- I controlli reattivi consentono di porre rimedio ai possibili scostamenti rispetto alle linee di base di sicurezza.

Sebbene l'IR sia generalmente visualizzato sotto il componente dei controlli reattivi, questi dipendono e sono influenzati dagli altri componenti. Ad esempio, i controlli di sicurezza di direzione e prevenzione aiutano a stabilire una linea di base, in modo da poter monitorare e indagare su eventuali deviazioni da tale linea di base. Questo approccio non solo elimina il rumore, ma contribuisce anche a una progettazione di sicurezza difensiva.

# Fondamenti della risposta agli incidenti

Tutti gli utenti AWS all'interno di un'organizzazione devono avere una conoscenza di base dei processi di risposta agli incidenti di sicurezza e il personale di sicurezza deve comprendere a fondo come reagire ai problemi di sicurezza. L'esperienza e la formazione sono fondamentali per un programma di risposta agli incidenti nel cloud, prima di gestire un evento di sicurezza. La base di un programma di successo di risposta agli incidenti nel cloud è educare, preparare,  simulare e iterare.

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

- Educare il personale che si occupa delle operazioni di sicurezza e della risposta agli incidenti in merito alle tecnologie cloud e al modo in cui l'organizzazione intende utilizzarle.
- Preparare il team di risposta agli incidenti a rilevare e rispondere agli incidenti nel cloud abilitando le funzionalità di rilevamento e garantendo un accesso appropriato agli strumenti e ai servizi cloud necessari. Inoltre, prepara i runbook necessari, sia manuali che automatizzati, per garantire risposte affidabili e coerenti. Collabora con altri team per stabilire le operazioni di base previste e utilizza tali conoscenze per identificare le divergenze rispetto alle operazioni normali.
- Simulare eventi di sicurezza previsti e imprevisti all'interno dell'ambiente cloud per comprendere l'efficacia della preparazione.
- Iterare sull'esito della simulazione per migliorare il livello di risposta, ridurre il time-to-value e ridurre ulteriormente il rischio.

# Istruzione

Argomenti



## Responsabilità condivisa

La responsabilità per la sicurezza e la conformità è condivisa tra te e AWS. Tale modello condiviso riduce l'onere operativo del cliente, dato che AWS rende operativi, gestisce e controlla tutti i componenti, dal sistema operativo host al livello di virtualizzazione fino alla sicurezza fisica delle strutture in cui operano i servizi.

Sei responsabile della gestione dei sistemi operativi guest (inclusi aggiornamenti e patch di sicurezza) e del software applicativo, nonché della configurazione dei controlli di sicurezza forniti da AWS, come gruppi di sicurezza, liste di controllo accessi alla rete e gestione delle identità e degli accessi. I clienti devono valutare con attenzione i servizi utilizzati, dato che le loro responsabilità variano in base ai servizi utilizzati, all'integrazione di tali servizi nel loro ambiente IT e alle leggi e ai regolamenti applicabili. La Figura 2 mostra una rappresentazione tipica del modello di responsabilità condivisa applicato ai servizi infrastrutturali, come Amazon Elastic Compute Cloud (Amazon EC2). Divide la maggior parte delle responsabilità in due categorie: sicurezza del cloud (gestita da AWS) e sicurezza nel cloud (gestita dal cliente). Le responsabilità possono cambiare a seconda dei servizi utilizzati. Per servizi astratti come Simple Storage Service (Amazon S3) e Amazon DynamoDB, AWS opera al livello dell'infrastruttura, il sistema operativo e le piattaforme e i clienti accedono agli endpoint per archiviare e recuperare i dati. I clienti sono responsabili della gestione dei dati (incluse le opzioni di crittografia), di classificare le risorse e utilizzare gli strumenti IAM per applicare le autorizzazioni appropriate.

Tuttavia, il modello di responsabilità condivisa cambia con l'aggiunta di container e altri servizi che spostano il modello operativo al fornitore di servizi. Man mano che ci spostiamo a sinistra del modello operativo, lontano da IaaS e data center e verso PaaS, la responsabilità del fornitore di servizi aumenta. Un cliente ha meno responsabilità nel cloud e più facilità a operare quando utilizza la migrazione a sinistra del grafico. Notare le seguenti figure e le differenze nella capacità di operare

o funzionare nel cloud. Man mano che la responsabilità condivisa nel cloud cambia, cambiano anche le opzioni per la risposta agli incidenti o le indagini forensi. In qualità di cliente, mentre pianifichi la risposta agli incidenti, dovrai anche assicurarti di pianificare in base alle capacità che hai nel tuo modello operativo e di pianificare le possibili interazioni prima che si verifichino nel modello che hai scelto. La pianificazione e la comprensione di questi compromessi e la loro corrispondenza con le esigenze di governance è una fase cruciale nella risposta agli incidenti.

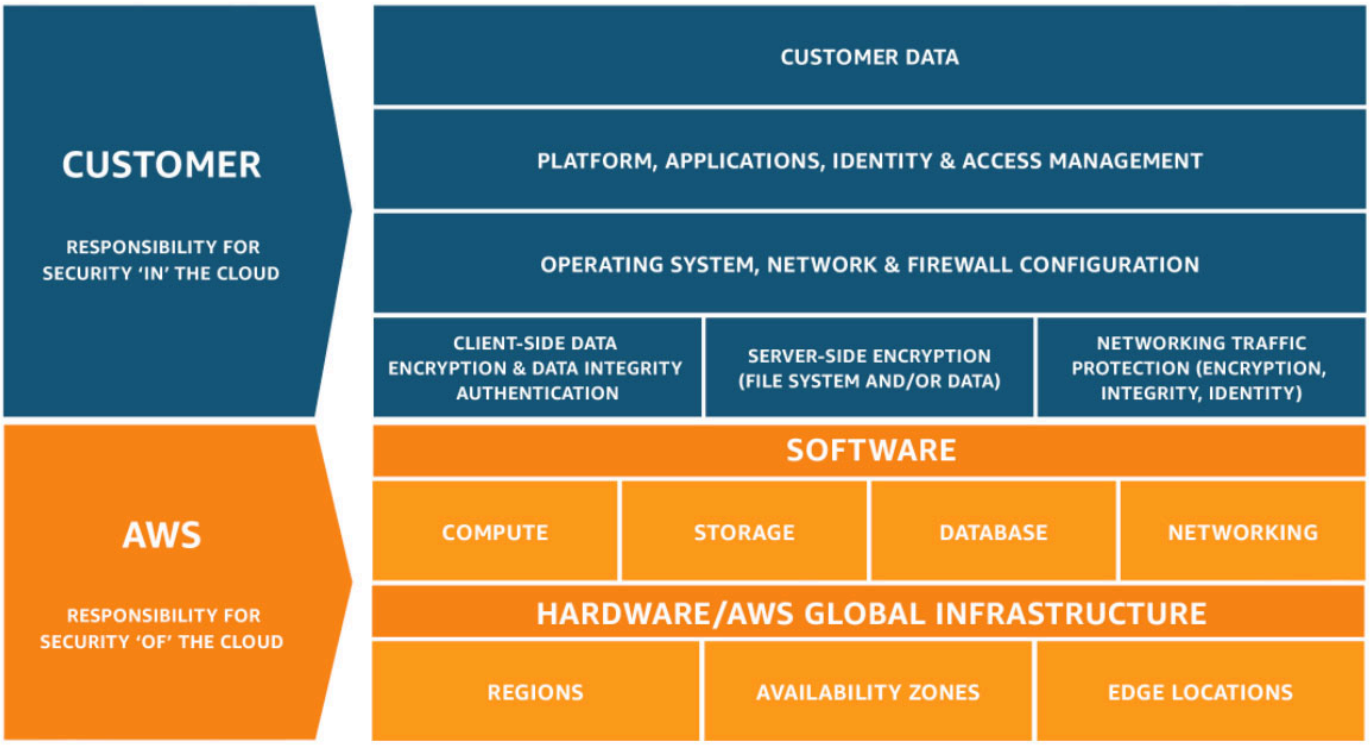


Figura 1: Modello di responsabilità condivisa

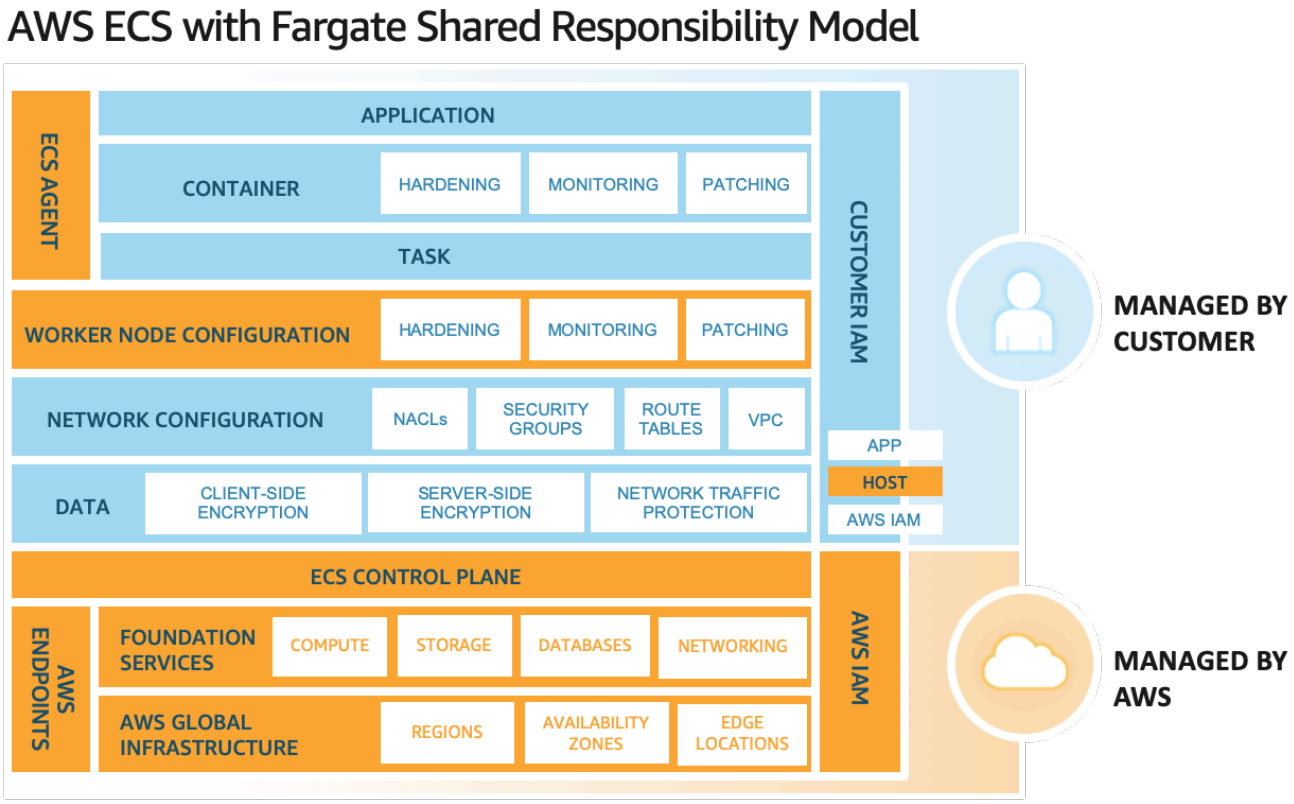


Figura 2: Amazon Elastic Container Service (Amazon ECS) con modello di responsabilità condivisa di tipo AWS Fargate

Oltre al rapporto diretto che hai con AWS, potrebbero esserci altre entità che hanno responsabilità nel tuo particolare modello di responsabilità. Ad esempio, potresti avere unità organizzative interne che si assumono la responsabilità di alcuni aspetti delle tue operazioni. Potresti anche avere partner o altre terze parti che sviluppano, gestiscono o operano su parte della tua tecnologia cloud.

La creazione di un appropriato runbook di risposta agli incidenti e forense che corrisponda al tuo modello operativo è estremamente importante. Il tuo successo dipende dalla comprensione dei tipi di strumenti che devi creare, o degli strumenti che devi acquistare, per il modello operativo che hai selezionato. Più la tua organizzazione comprende gli strumenti disponibili, più sarai preparato a soddisfare le esigenze del modello GRC (Governance Risk and Compliance) della tua azienda.

# Risposta agli incidenti nel cloud

## Progettazione degli obiettivi di risposta al cloud

Sebbene i processi e i meccanismi generali di risposta agli incidenti, come quelli definiti nella NIST SP 800-61 Computer Security Incident Handling Guide rimangano validi, ti consigliamo di considerare i seguenti obiettivi di progettazione specifici pertinenti per rispondere agli incidenti di sicurezza in un ambiente cloud:

- Definizione degli obiettivi di risposta: collabora con le parti interessate, i consulenti legali e la leadership dell'organizzazione per determinare l'obiettivo di risposta a un incidente. Alcuni obiettivi comuni includono il contenimento e la mitigazione del problema, il ripristino delle risorse interessate, la conservazione dei dati per le analisi forensi e l'attribuzione.
- Risposte fornite utilizzando il cloud: implementa i tuoi modelli di risposta dove si verificano l'evento e i dati.
- Individuazione dei dati esistenti e di quelli necessari: conserva registri, snapshot e altre prove copiandoli in un account cloud di sicurezza centralizzato. Utilizza tag, metadati e meccanismi che applicano le policy di conservazione. Ad esempio, puoi scegliere di utilizzare il comando dd di Linux o un equivalente di Windows per creare una copia completa dei dati a scopo investigativo.
- Utilizzo di meccanismi di ridistribuzione: se un'anomalia di sicurezza può essere attribuita a una configurazione errata, la correzione potrebbe essere semplicemente rimuovere la varianza ridistribuendo le risorse con la configurazione corretta. Quando possibile, rendi i meccanismi di risposta sicuri in modo da eseguirli più di una volta e in stati sconosciuti.
- Automatizzazione laddove possibile: quando si verificano problemi o incidenti ripetuti, costruisci meccanismi che verifichino e rispondano a situazioni comuni a livello di programmazione. Utilizza le risposte umane per incidenti unici, nuovi e sensibili.
- Scelta di soluzioni scalabili: cerca di soddisfare la scalabilità dell'approccio dell'organizzazione al cloud computing e riduci le tempistiche tra rilevamento e risposta.
- Individuazione delle lacune e miglioramento del processo: quando individui lacune nel processo, negli strumenti o nelle persone, implementa piani per correggerle. Le simulazioni sono metodi sicuri per individuare le lacune e migliorare i processi.

Gli obiettivi di progettazione del NIST ricordano di rivedere l'architettura per la capacità di condurre sia la risposta agli incidenti che il rilevamento delle minacce. Mentre pianifichi l'implementazione del cloud, pensa a come rispondere a un incidente o a un evento 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 dovrebbero essere resi disponibili all'incident responder dalla pipeline di implementazione e non dovrebbero essere statici, poiché ciò comporterebbe un rischio maggiore.

# Incidenti di sicurezza del cloud

Argomenti



## Ambiti degli incidenti

Vi sono tre ambiti tra le responsabilità del cliente, dove potrebbero verificarsi incidenti di sicurezza: servizio, infrastruttura e applicazione. La differenza tra gli ambiti è correlata agli strumenti utilizzati in risposta. Considera questi ambiti:

- Ambito di servizio: incidenti nell'ambito del servizio influiscono su un account di un cliente AWS, sulle autorizzazioni IAM, sui metadati delle risorse, sulla fatturazione, e su altre aree. Un evento nell'ambito del servizio è un evento a cui si risponde solo con i meccanismi API AWS, oppure dove si hanno cause associate alla configurazione o alle autorizzazioni della risorsa, e potrebbe avere una registrazione correlata orientata al servizio.
- Ambito dell'infrastruttura: gli incidenti nell'ambito dell'infrastruttura includono dati o attività correlate alla rete, come il traffico alle istanze Amazon EC2 all'interno del VPC, i processi e i dati nelle istanze Amazon EC2 e altre aree, come i container o altri servizi futuri. La risposta agli eventi dell'ambito dell'infrastruttura spesso coinvolge il recupero, il ripristino o l'acquisizione di dati relativi all'incidente per l'analisi forense. Probabilmente include l'interazione con il sistema operativo di un'istanza e, in alcuni casi, potrebbe anche coinvolgere i meccanismi API AWS.
- Ambito dell'applicazione: gli incidenti nell'ambito dell'applicazione avvengono nel codice dell'applicazione o nel software implementato ai servizi o all'infrastruttura. Questo ambito dovrebbe essere incluso nei runbook di rilevamento e risposta alle minacce del cloud, e potrebbe incorporare risposte simili a quelle dell'ambito dell'infrastruttura. Con un'architettura delle applicazioni appropriata e accurata, puoi gestire questo ambito con gli strumenti cloud utilizzando strumenti digitali forensi automatizzati, il ripristino e l'implementazione.

In questi ambiti, devi considerare gli attori che potrebbero agire contro l'account, le risorse o i dati. Sia interno che esterno, utilizza un framework di rischio per determinare quali sono i rischi specifici per l'organizzazione e preparati di conseguenza.

Nell'ambito del servizio, operi per raggiungere i tuoi obiettivi esclusivamente con le API di AWS. Per esempio, la gestione di un incidente di divulgazione di dati da un bucket Simple Storage Service (Amazon S3) coinvolge le chiamate API per recuperare la policy del bucket, analizzando i registri di accesso S3 e possibilmente esaminando i registri di AWS CloudTrail. In questo esempio, è improbabile che la tua indagine coinvolga gli strumenti per l'analisi forense dei dati o gli strumenti di analisi del traffico di rete.

Nell'ambito dell'infrastruttura, puoi utilizzare una combinazione di API AWS e un software conosciuto di disciplina digitale forense/risposta agli incidenti (DFIR), all'interno del sistema operativo di una workstation, come un'istanza Amazon EC2 che hai preparato per l'attività IR. Gli incidenti dell'ambito dell'infrastruttura potrebbero coinvolgere l'analisi delle acquisizioni di pacchetti di rete, i blocchi di disco in un volume Amazon Elastic Block Store (Amazon EBS), o la memoria volatile acquisita da un'istanza.

## Indicatori degli eventi di sicurezza nel cloud

Esistono molti eventi di sicurezza che potresti non classificare come incidenti, ma potrebbe essere comunque prudente esaminarli. Per rilevare eventi relativi alla sicurezza nell'ambiente AWS Cloud, puoi utilizzare questi meccanismi. Sebbene non sia un elenco esaustivo, si considerino i seguenti esempi di alcuni potenziali indicatori:

- Registri e monitor: verifica i registri AWS (ad esempio Amazon CloudTrail, i registri di accesso di Simple Storage Service (Amazon S3) e i flussi di log del VPC) e i servizi di monitoraggio della sicurezza (come Amazon GuardDuty, Amazon Detective, AWS Security Hub e Amazon Macie). Inoltre, utilizza monitoraggi come i controlli dell'integrità di Amazon Route 53 e gli allarmi di Amazon CloudWatch. Allo stesso modo, utilizza gli eventi di Windows, i registri syslog di Linux e altri registri specifici delle applicazioni che puoi generare nelle applicazioni e accedi ad Amazon CloudWatch, utilizzando gli agenti CloudWatch.
- Attività di fatturazione: un cambiamento improvviso nell'attività di fatturazione può indicare un evento di sicurezza.
- Intelligence sulle minacce: se si sottoscrive un feed di intelligence sulle minacce di terze parti, è possibile correlare tali informazioni con altri strumenti di registrazione e monitoraggio per identificare potenziali indicatori di eventi.

- Strumenti per i partner: i partner nella rete dei partner AWS (APN) offrono centinaia di prodotti leader del settore che possono aiutarti a raggiungere i tuoi obiettivi di sicurezza. Per ulteriori informazioni, consulta la sezione relativa alle soluzioni dei partner per la sicurezza e Soluzioni per la sicurezza nel Marketplace AWS.
- AWS Outreach: AWS Support potrebbe contattarti se identifichiamo attività illecite o dannose. Per ulteriori informazioni, consulta la sezione relativa alla risposta AWS a uso illecito e a compromissioni.
- Contatto occasionale: poiché possono essere i tuoi clienti, i tuoi sviluppatori o altro personale della tua organizzazione a notare qualcosa di insolito, è importante avere un metodo conosciuto e ben pubblicizzato per contattare il team di sicurezza. Le scelte più diffuse includono sistemi di ticket, indirizzi e-mail di contatto e moduli Web. Se l'organizzazione lavora con il pubblico in generale, potrebbe essere necessario anche un meccanismo di contatto di sicurezza rivolto al pubblico.

Uno degli strumenti offerti da AWS per l'automazione e il rilevamento è AWS Security Hub. Security Hub offre una visione completa degli avvisi di sicurezza ad alta priorità e dello stato di conformità tra gli account AWS in un'unica posizione, consentendo una migliore visibilità di questi indicatori. AWS Security Hub non è un software SIEM (Security Information and Event Management) e non archivia i dati dei registri, ma aggrega, organizza e assegna priorità agli avvisi o ai risultati di sicurezza provenienti da più servizi AWS. Security Hub offre anche la possibilità di creare informazioni dettagliate personalizzate che possono derivare da più fonti. Ciò offre al team delle operazioni di sicurezza opzioni e informazioni dettagliate su ulteriori informazioni quando si verifica un evento. Security Hub monitora di continuo il tuo ambiente usando i controlli di conformità automatizzati basati sulle best practice di AWS e gli standard di settore che la tua organizzazione segue.

Puoi anche intervenire su questi risultati di sicurezza e conformità verificandoli con Amazon Detective o Amazon Athena, o utilizzando le regole di Amazon CloudWatch Events o di Event Bus per inviare i risultati a strumenti di ticketing, chat, SIEM, Security Orchestration Automation and Response (SOAR) e di gestione degli incidenti o a playbook di correzione personalizzati. L'automazione basata sugli eventi consente di rispondere automaticamente a incidenti o eventi che si verificano. Questo approccio modifica la sicurezza e il modo in cui gestisci gli eventi nel cloud rispetto agli ambienti On-Premise.

## Comprendere le funzionalità del cloud

AWS offre un'ampia gamma di funzionalità di sicurezza che è possibile utilizzare per analizzare gli eventi di sicurezza nei vari ambiti. Ad esempio, AWS fornisce una serie di meccanismi di

registrazione, come i registri di AWS CloudTrail, Amazon CloudWatch Logs, i registri di accesso di Simple Storage Service (Amazon S3) e altro ancora. È necessario considerare i servizi che si stanno utilizzando e assicurarsi di aver abilitato i registri relativi a tali servizi. AWS offre anche una soluzione di registrazione centralizzata, che può aiutare a capire come centralizzare e archiviare i tipi più comuni di registro nel cloud. Dopo aver abilitato queste fonti di registrazione, è necessario decidere come analizzarle, ad esempio utilizzando Amazon Athena per eseguire query sui registro conservati nei bucket Simple Storage Service (Amazon S3).

Inoltre, esistono numerosi prodotti dei partner APN che possono semplificare il processo durante l'analisi di questi registri, come quelli descritti nel programma APN Security Competency. Esistono anche diversi servizi AWS che possono aiutare a ottenere informazioni dettagliate preziose su questi dati, come Amazon GuardDuty (un servizio di rilevamento delle minacce) e AWS Security Hub, che può fornire una visione completa degli avvisi di stato ad alta priorità sulla sicurezza e la conformità su tutti gli account AWS. Inoltre, Amazon Detective raccoglie i dati dei registri dalle risorse AWS e utilizza il machine learning, l'analisi statistica e la teoria dei grafi per aiutarti a identificare la causa principale di potenziali problemi di sicurezza o attività sospette. Per ulteriori informazioni sulle ulteriori funzionalità del cloud che puoi sfruttare durante le indagini, consulta l'Appendice A: definizioni delle capacità cloud.

Argomenti



## Privacy dei dati

Sappiamo che i clienti hanno a cuore la privacy e la sicurezza dei dati e quindi implementiamo controlli tecnici e fisici responsabili e sofisticati progettati per impedire l'accesso non autorizzato o la divulgazione dei contenuti dei clienti. Conservare intatta la fiducia che i clienti ripongono in noi è un impegno costante. Puoi trovare ulteriori informazioni relative all'impegno di AWS per la privacy dei dati nella pagina Domande frequenti sulla privacy dei dati.

Questi controlli intenzionali e autoimposti limitano la capacità di AWS di fornire assistenza nella risposta all'interno dell'ambiente di un cliente. Per questo motivo, concentrarsi sulla comprensione e sulla creazione di funzionalità all'interno del modello di responsabilità condivisa è fondamentale per il successo in AWS Cloud. Sebbene sia importante abilitare le funzionalità di registrazione e monitoraggio negli account AWS prima che si verifichi un incidente, ci sono altri aspetti nella risposta agli incidenti che sono fondamentali per un programma di successo.

### Privacy dei dati del cliente - California

Il California Consumer Privacy Act del 2018 (CCPA) concede ai "consumatori vari diritti in relazione alle informazioni personali relative al consumatore detenute da un'azienda" che è soggetta al CCPA. Per informazioni sulle policy di privacy e sicurezza dei dati di AWS in relazione ai clienti soggetti al CCPA, consulta il whitepaper Preparing for the California Consumer Privacy Act per indicazioni.

### Regolamento generale sulla protezione dei dati:

Il Regolamento generale sulla protezione dei dati (GDPR) è una legge europea sulla privacy (Regolamento 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016) che è entrato in vigore il 25 maggio 2018. Il GDPR sostituisce la Direttiva UE sulla protezione dei dati (Direttiva 95/46/CE) e il suo scopo è di armonizzare le leggi relative alla protezione dei dati in tutta l'Unione europea (UE) con l'applicazione di un'unica legge vincolante in ogni stato membro della UE. Per informazioni sulla conformità di AWS in relazione al GDPR, consulta il whitepaper Navigating GDPR Guidance on AWS.

## Risposta di AWS a usi illeciti e compromissioni

Le attività illecite sono comportamenti osservati delle istanze dei clienti AWS o di altre risorse che sono dannosi, offensivi, illegali o che potrebbero danneggiare altri siti Internet. AWS collabora con te per rilevare e risolvere attività sospette e dannose nelle risorse AWS. Comportamenti inaspettati o sospetti delle risorse possono indicare che le risorse AWS sono state compromesse, il che segnala potenziali rischi per l'azienda. Ricorda che hai metodi di contatto alternativi nel tuo account AWS. Assicurati di utilizzare le best practice per l'aggiunta di contatti, sia per la sicurezza che per la fatturazione. Sebbene l'e-mail dell'account root sia l'obiettivo principale della comunicazione da parte di AWS, AWS comunica anche problemi di sicurezza e problemi di fatturazione agli indirizzi e-mail secondari. L'aggiunta di un indirizzo e-mail indirizzato a una sola persona significa che hai aggiunto un singolo punto di errore all'account AWS. Assicurati di aver aggiunto ai tuoi contatti almeno una lista di distribuzione.

AWS rileva gli usi illeciti nelle risorse utilizzando meccanismi come:

- Monitoraggio degli eventi interni di AWS.
- Informazioni sulla sicurezza esterna nello spazio degli indirizzi di rete AWS.
- Segnalazioni di uso illecito di Internet nelle risorse AWS.

Sebbene il team AWS di risposta all'uso illecito monitori e chiuda le attività non autorizzate in esecuzione su AWS, la maggior parte delle segnalazioni di uso illecito si riferisce a clienti che hanno attività legittime su AWS. Alcuni esempi di cause comuni di uso illecito involontario includono:

- Risorsa compromessa: un'istanza Amazon EC2 senza patch potrebbe essere infettata e diventare un agente botnet.
- Uso illecito involontario: un Web crawler eccessivamente aggressivo potrebbe essere classificato come un attacco denial-of-service da parte di alcuni siti internet.
- Uso illecito secondario: un utente finale del servizio fornito da un cliente AWS potrebbe pubblicare file di malware su un bucket Simple Storage Service (Amazon S3) pubblico.
- False segnalazioni: a volte gli utenti di Internet segnalano erroneamente attività legittime come uso illecito.

AWS si impegna a collaborare con i clienti AWS per prevenire, rilevare e mitigare gli l'uso illecito e per difendersi da future ricorrenze. Ti invitiamo a leggere la Policy sull'utilizzo accettabile di AWS, che descrive gli usi vietati dei servizi Web offerti da Amazon Web Services e dalle sue affiliate. Per supportare una risposta tempestiva alle notifiche di uso illecito da parte di AWS, assicurati che le informazioni di contatto del tuo account AWS siano accurate. Quando ricevi un avviso di uso illecito di AWS, il personale addetto alla sicurezza e operativo deve indagare immediatamente sulla questione. Un ritardo può prolungare l'impatto sulla reputazione e implicazioni legali per te e gli altri. Ancora più importante, la risorsa usata in modo illecito implicata potrebbe essere compromessa da utenti malintenzionati e ignorare la compromissione potrebbe aumentare i danni all'azienda.

# Preparazione: personale

I processi automatizzati consentono alle organizzazioni di dedicare più tempo a concentrarsi sulle misure per aumentare la sicurezza dell'ambiente cloud e delle applicazioni. La risposta automatizzata agli incidenti offre inoltre più tempo al personale per correlare eventi, eseguire simulazioni, ideare nuove procedure di risposta, eseguire ricerche, sviluppare nuove competenze e testare o costruire nuovi strumenti. Nonostante l'aumento dell'automazione, gli analisti e i risponditori all'interno di un'organizzazione di sicurezza hanno ancora molto da fare. I team omogenei possono creare punti ciechi, quindi è essenziale costruire un team diversificato che offra diversi sistemi di pensiero, prospettive culturali ed esperienze lavorative e di vita in situazioni fluide complesse. Una delle cose di maggior impatto che possiamo fare durante la pianificazione degli eventi è assicurarci che la diversità sia integrata nei team e nei piani di risposta. Un team che comprende diverse prospettive può potenzialmente identificare i punti ciechi che potrebbero non essere stati rilevati e identificare soluzioni che altrimenti non sarebbero state considerate.

Argomenti



## Definizione di ruoli e responsabilità

Le competenze e i meccanismi di risposta agli incidenti sono molto importanti quando si gestiscono eventi nuovi o su larga scala. Questi eventi si basano sugli standard scritti che il team ha sviluppato e sull'esperienza pratica del team. Poiché non possiamo prevedere o codificare tutte le potenziali direzioni che può prendere un evento, ci affidiamo all'automazione per attività semplici e ripetitive, come la raccolta di memoria delle istanze o registri diagnostici, e lasciamo che le persone prendano le decisioni difficili. La gestione di eventi di sicurezza poco chiari richiede disciplina tra le organizzazioni, propensione a operazioni decisive e capacità di ottenere risultati. All'interno della struttura organizzativa, dovrebbero esserci molte persone responsabili, affidabili, consultate o tenute informate durante un incidente, come i rappresentanti delle risorse umane (HR), il team dirigenziale e quello legale. Considera questi ruoli e responsabilità e se devono essere coinvolte terze parti. Si noti che in molte aree geografiche esistono leggi locali che regolano ciò che si può e non si può fare. Sebbene possa sembrare un'operazione burocratica costruire un grafico RACI (Responsible,

Accountable, Consulted, Informed), ciò consente una comunicazione rapida e diretta e delinea chiaramente la leadership nelle diverse fasi dell'evento.

I partner affidabili possono essere coinvolti nell'indagine o nella risposta e forniscono ulteriori competenze e un prezioso controllo. Quando non hai queste competenze nella tuo team, potresti voler assumere una parte esterna per assistenza. Se assumi una parte esterna, assicurati che questa addestri i membri del team. Quando queste parti esterne lavorano con i tuoi sviluppatori e operatori interni, possono ampliare le competenze dei membri del team e le nuove competenze possono essere preziose per il programma IR in futuro.

Durante un incidente, includere i proprietari e gli sviluppatori delle applicazioni e delle risorse interessate è fondamentale perché sono SME in grado di fornire informazioni e contesto. Assicurati di fare pratica e di costruire relazioni con gli sviluppatori e i proprietari delle applicazioni prima di affidarti alla loro competenza per la risposta agli incidenti. Ai proprietari delle applicazioni o alle PMI può essere richiesto di agire in situazioni in cui l'ambiente non è familiare, presenta una complessità imprevista o in cui i team di risposta non hanno accesso. Gli SME delle applicazioni dovrebbero esercitarsi e sentirsi a proprio agio nel lavorare con il team IR.

## Fornire formazione

Per ridurre le dipendenze e ridurre il tempo di risposta, assicurati che i team di sicurezza e i team di risposta siano informati sui servizi cloud e abbiano opportunità di esercitarsi direttamente con le piattaforme cloud specifiche utilizzate dalla tua organizzazione. Parte di questa formazione deriva dalla costruzione del team e dalla creazione dei runbook che avviene all'inizio del processo. Includendo quante più persone possibile nella fase iniziale della formazione dei runbook, fornisci una migliore comprensione ai team interni. Questa formazione diventa più reale quando i team iniziano a seguire i runbook negli esercizi di simulazione.

AWS e altre terze parti forniscono anche workshop sulla sicurezza online (AWS Security Workshops) che puoi scaricare e utilizzare. L'organizzazione può trarre vantaggio dalla formazione aggiuntiva del personale per apprendere le competenze di programmazione, i processi di sviluppo (inclusi i sistemi di controllo delle versioni e le pratiche di implementazione) e l'automazione dell'infrastruttura.

AWS offre una serie di opzioni di formazione e percorsi di apprendimento tramite la formazione digitale, la formazione in aula, i partner APN e le certificazioni. Per ulteriori informazioni, consulta AWS Training & Certification.

# Definizione dei meccanismi di risposta

Il tuo meccanismo di risposta dipende dal modello di governance, rischio e conformità (GRC). Idealmente, il modello GRC viene costruito prima di pianificare la risposta agli incidenti. Se non hai iniziato a creare un GRC, è un primo passaggio necessario per costruire un buon meccanismo di risposta agli incidenti. Quando definisci come affrontare la risposta agli incidenti nel cloud, insieme ad altri team (ad esempio il consulente legale, la leadership dell'organizzazione, le parti interessate e altri), devi comprendere cosa hai a disposizione e quali sono le necessità. Identifica le parti interessate e i contatti pertinenti e assicurati di avere un accesso appropriato per fornire la risposta necessaria.

Sebbene il cloud possa fornirti maggiore visibilità e funzionalità attraverso le API dei servizi, il modello GRC ti mostra come utilizzarle nella risposta. Identifica i numeri di account AWS del team, gli intervalli di indirizzi IP dei cloud privati virtuali (VPC), i diagrammi di rete corrispondenti, i registri, le posizioni e le classificazioni dei dati. Molti di questi processi tecnologici sono inclusi nella sezione Preparazione - Tecnologia. Quindi, inizia a documentare le procedure di risposta agli incidenti, spesso indicate come procedure o runbook, che definiscono i passaggi per l'indagine e la risoluzione di un incidente.

# Creazione di una cultura della sicurezza ricettiva e adattiva

In AWS, abbiamo imparato che i nostri clienti e i nostri team interni hanno più successo quando i team di sicurezza sono fattori abilitanti di cooperazione per la loro attività e i suoi sviluppatori, che promuovono una cultura che assicura che tutte le parti interessate cooperino e crescano per mantenere una posizione di sicurezza agile e altamente reattiva. Sebbene il miglioramento della cultura della sicurezza della tua organizzazione non sia l'argomento di questo documento, puoi ottenere informazioni pertinenti dal personale non addetto alla sicurezza se ritiene che il team addetto alla sicurezza è ricettivo. Quando il team di sicurezza è aperto e accessibile, con il supporto della leadership, è più probabile che riceva notifiche aggiuntive e tempestive, cooperazione e risposte agli eventi di sicurezza.

In alcune organizzazioni, il personale potrebbe temere problemi se segnala un problema di sicurezza. A volte semplicemente non sanno come segnalare un problema. In altri casi, potrebbero non voler perdere tempo o potrebbero essere imbarazzati nel segnalare qualcosa come un incidente di sicurezza che in seguito viene ritenuto non essere un problema. Dal team manageriale in giù, è importante promuovere una cultura dell'accettazione e invitare tutti a far parte della sicurezza dell'organizzazione. Fornire a chiunque un canale chiaro per aprire un ticket di gravità elevata, ogni

volta che ritiene che possa esserci un potenziale rischio o minaccia. Accogli queste notifiche con una mente aperta e entusiasta, ma soprattutto, chiarisci al personale non addetto alla sicurezza che tali notifiche sono accettate di buon grado. Sottolinea che preferiresti essere informato in modo eccessivo di potenziali problemi, piuttosto che non ricevere alcuna notifica. È molto meglio per uno sviluppatore comunicare il proprio errore, piuttosto che un ricercatore segnali il problema in un articolo pubblico.

Queste notifiche offrono preziose opportunità per svolgere indagini reattive in condizioni di stress. Possono fungere da importante circuito di feedback mentre sviluppi le procedure di risposta.

# Previsione di risposta

Poiché è impossibile prevedere tutti i potenziali eventi, è necessario continuare a fare affidamento sull'analisi umana. Prendersi il tempo necessario per formare accuratamente il personale e preparare la propria organizzazione aiuta ad anticipare gli imprevisti; tuttavia, l'organizzazione non deve prepararsi isolatamente. La collaborazione con partner di sicurezza affidabili per identificare eventi di sicurezza imprevisti offre alle organizzazioni il vantaggio di una maggiore visibilità e informazioni dettagliate.

## I partner e la finestra di risposta

Il percorso verso il cloud è particolare per ogni organizzazione. Tuttavia, ci sono modelli e pratiche che altre organizzazioni hanno già affrontato e che un partner di sicurezza affidabile può portare alla tua attenzione. Ti invitiamo a identificare i partner APN di sicurezza AWS esterni in grado di fornirti competenze e una prospettiva diversa per potenziare le capacità di risposta. I partner di sicurezza affidabili possono aiutarti a identificare potenziali rischi o minacce che potresti non conoscere.

Nel 1955, Joseph Luft e Harrington Ingham crearono la finestra di Johari, un esercizio per la mappatura dei tratti alle categorie. La finestra è rappresentata come una griglia composta da quattro quadranti, simile al diagramma seguente.

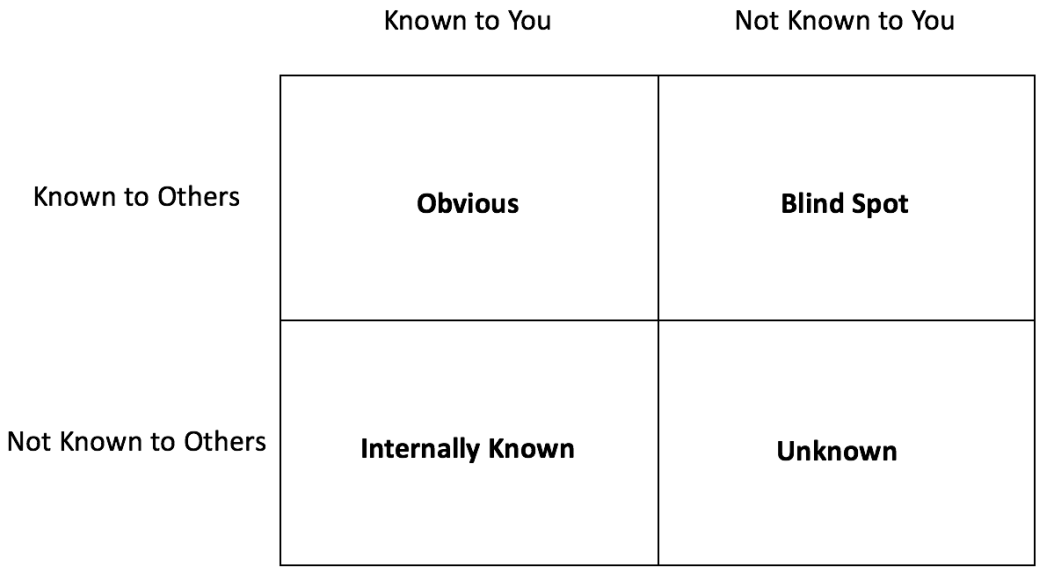


Figura 3: Finestra di Johari modificata per la risposta agli incidenti

Sebbene la finestra di Johari non sia destinata alla sicurezza delle informazioni, possiamo adattare il concetto per usarlo come un semplice modello mentale per considerare la difficoltà nel valutare le minacce di un'organizzazione. Nel nostro concetto modificato, i quattro quadranti sono:

- Ovvio: rischio di cui sia il team che il partner APN sono a conoscenza.
- Conosciuto internamente: rischio con cui il team ha familiarità, ma con il quale il tuo partner APN non ne ha. Ciò potrebbe significare che hai competenze conoscenze all'interno dell'organizzazione.
- Punto cieco: rischio con cui il partner APN ha familiarità, ma con il quale il team non ne ha.
- Sconosciuto: rischio che né tu né il partner APN avete familiarità.

Sebbene questo diagramma sia semplice, rappresenta il valore che è possibile ottenere avendo un partner APN di fiducia. Soprattutto, potrebbero esserci punti ciechi di cui non sei a conoscenza, ma che un partner APN con la giusta esperienza può sottoporre alla tua attenzione. Sebbene entrambi possiate avere familiarità con questi rischi nel quadrante ovvio, il partner APN potrebbe consigliare controlli e soluzioni che non conosci. Inoltre, sebbene potresti portare questi rischi nel quadrante noto internamente all'attenzione del partner APN, egli potrebbe anche essere in grado di identificare controlli ottimizzati per mitigare tale rischio. Mentre ti metti alla prova per il miglioramento, contatta il partner APN per ottenere una consulenza esperta.

# Rischio sconosciuto

Se ti sei concentrato sulla personalizzazione degli avvisi, sul miglioramento delle procedure di risposta agli incidenti con l'automazione e sul miglioramento delle difese di sicurezza, ti starai chiedendo cosa migliorare oltre a questi aspetti. Potresti essere curioso di conoscere il rischio sconosciuto, come rappresentato nella categoria sconosciuto nella Figura 3. È possibile ridurre il rischio sconosciuto attraverso i seguenti metodi:

- Definire le affermazioni di sicurezza: quali sono alcune verità che puoi affermare? Quali sono le primitive della sicurezza che dovrebbero assolutamente essere vere nel tuo ambiente? Definirle chiaramente consente di cercare il contrario. Si tratta di qualcosa che è più facile da fare nelle prime fasi del percorso verso il cloud, piuttosto che tentare di decodificare le asserzioni di sicurezza in un secondo momento.
- Istruzione, comunicazione e ricerca: crea esperti di sicurezza cloud nel tuo personale o includi partner esperti per aiutarti a controllare il tuo ambiente. Sfida i tuoi presupposti e diffida dei ragionamenti superficiali. Crea circuiti di feedback nei tuoi processi e offri ai team di tecnici i meccanismi per comunicare con i team di sicurezza. È inoltre possibile ampliare l'approccio per monitorare le liste di distribuzione di sicurezza e la divulgazione delle informazioni sulla sicurezza.
- Riduzione della superficie d'attacco: migliora la difesa per evitare rischi e concediti più tempo per attacchi sconosciuti. Blocca e rallenta gli aggressori e costringili a fare rumore.
- Intelligence sulle minacce: sottoscrivi un feed continuo di minacce, rischi e indicatori attuali e pertinenti provenienti da tutto il mondo.
- Avvisi: genera notifiche che avvisano di attività insolite, dannose o costose. Ad esempio, è possibile creare una notifica per le attività che si verificano in regioni o servizi che non si utilizzano.
- Machine Learning: utilizza il machine learning per identificare anomalie complesse per un'organizzazione specifica o per singoli individui. Per aiutarti a identificare comportamenti insoliti, puoi anche profilare le normali caratteristiche delle reti, utenti e sistemi.

L'intelligence sulle minacce diventa l'argomento principale quando si considerano i punti ciechi e le incognite sconosciute. La finestra di Johari mostra come classificare ciò che conosci e non conosci, ma l'intelligence sulle minacce mostra come considerare ciò che ancora non conosci. L'intelligence sulle minacce è una disciplina che aiuta le aziende a vedere oltre il modello delle minacce, per trovare minacce che l'azienda potrebbe non ancora conoscere.

In generale, l'intelligence sulle minacce comprende:

1. Trovare nuove minacce.
2. Definizione di nuovi modelli.
3. Definizione di nuove tecniche di acquisizione automatizzata.
4. Ripetizione di questi processi.

Sebbene questo tipo di pratica possa essere utile, la cura e il mantenimento di un team di intelligence sulle minacce può gravare eccessivamente su molte aziende, anche grandi. Alla fine, la domanda diventa quella di abbinare il modello di minaccia, le dimensioni e le avversità di rischio. Considerare queste domande:

- Il tuo modello di minaccia è abbastanza diverso dal verticale standard in cui si trova l'azienda?
- La propensione al rischio è sufficientemente bassa da richiedere un team del genere?
- È fiscalmente corretto gestire un team per la tua azienda?
- Il tuo profilo di rischio è abbastanza interessante da attirare talenti ragionevoli per la tua causa?

Se rispondi no a una di queste domande, molto probabilmente dovresti trovare un partner di intelligence sulle minacce. Questo servizio è offerto in modo competitivo da molte aziende grandi e molto note.

AWS ti fornisce gli strumenti e i servizi per gestire autonomamente questi problemi. L'utilizzo del machine learning per identificare modelli dannosi è un settore di studio molto approfondito, con modelli implementati da clienti, servizi professionali AWS, partner APN e tramite servizi AWS come Amazon GuardDuty e Amazon Macie. Alcuni di questi modelli sono stati illustrati durante le sessioni della conferenza AWS re:Invent. Per ulteriori informazioni, consulta la sezione Media di questo whitepaper.

I clienti stanno inoltre espandendo i loro data lake tradizionalmente incentrati sul business per sfruttare modelli di architettura simili quando sviluppano data lake di sicurezza. I team addetti alle operazioni di sicurezza stanno inoltre espandendo il loro uso dei tradizionali strumenti di registrazione e monitoraggio, come i pannelli di controllo Amazon OpenSearch Service e OpenSearch, alle architetture dei Big Data.

Questi clienti stanno raccogliendo dati interni da registri di eventi AWS CloudTrail, flussi di log VPC, registri di accesso di Amazon CloudFront, registri di database e registri delle applicazioni e quindi combinano questi dati con dati pubblici e di intelligence sulle minacce. Con questi preziosi dati, i clienti hanno ampliato per includere competenze di Data Science e di data engineering nei team

operativi di sicurezza per sfruttare strumenti come Amazon EMR, Amazon Kinesis Data Analytics, Amazon Redshift, Amazon QuickSight, AWS Glue, Amazon SageMaker e Apache MXNet su AWS per costruire soluzioni personalizzate che identificano e prevedono anomalie specifiche dell'azienda.

Infine, consulta la sezione Security Partner Solutions per centinaia di prodotti leader del settore dei partner APN che sono equivalenti, identici o integrati con i controlli esistenti nei tuoi On-Premise. Questi prodotti integrano i servizi AWS esistenti per permettere di implementare un'architettura di sicurezza completa e un'esperienza più fluida nel cloud e negli ambienti locali.

# Preparazione - Tecnologia

Argomenti



## Preparazione dell'accesso agli account AWS

Durante un incidente, i team di risposta agli incidenti devono avere accesso all'ambiente e alle risorse coinvolte nell'incidente. Assicurati che i team dispongano dell'accesso appropriato per eseguire le loro attività prima che si verifichi un evento. È necessario conoscere il livello di accesso richiesto dai membri del team (ad esempio, quali tipi di operazioni potrebbero intraprendere) ed è necessario assegnare l'accesso in anticipo. Questo accesso deriva dalle policy di governance, gestione del rischio e conformità (GRC) dell'azienda. L'autenticazione e l'autorizzazione dei membri del team devono essere documentate e testate molto prima che si verifichi un evento per assicurarsi che possano fornire una risposta tempestiva senza ritardi. Per rispondere correttamente a un incidente, parte della preparazione dovrebbe essere una revisione di come sono disposti gli account AWS e come i ruoli tra account sono consentiti e organizzati.

In questa fase, è necessario lavorare a stretto contatto con sviluppatori, architetti, partner, team di governance e team di conformità per capire quale livello di accesso è necessario per gli interventi. Identifica e discuti la strategia degli account AWS e la strategia di identità cloud con gli architetti del cloud dell'organizzazione per capire quali metodi di autenticazione e autorizzazione sono configurati, ad esempio:

- Federazione: un utente assume un ruolo IAM in un account AWS da un provider di identità.
- Accesso tra più account: un utente assume un ruolo IAM tra più account AWS.
- Autenticazione: un utente si autentica come utente AWS IAM creato all'interno di un singolo account AWS.

Queste opzioni definiscono le scelte tecniche per l'autenticazione in AWS e il modo in cui è possibile ottenere l'accesso durante una risposta, ma alcune organizzazioni potrebbero fare affidamento su un altro team o un partner per fornire assistenza nella risposta. Gli account utente creati appositamente per rispondere a un incidente di sicurezza sono spesso privilegiati per fornire accesso sufficiente.

Pertanto, l'uso di questi account utente deve essere limitato, essi non devono essere utilizzati per le attività quotidiane.

Prima di creare nuovi meccanismi di accesso, collabora con i team del cloud per capire come sono organizzati e gestiti gli account AWS. Molti clienti utilizzano AWS Organizations per aiutare a gestire centralmente la fatturazione, condividere risorse tra gli account AWS e controllare l'accesso, la conformità e la sicurezza. Una caratteristica fondamentale di Organizations è che può essere sfruttato per applicare le policy di controllo dei servizi a gruppi di account, il che consente di ottenere la gestione delle policy su larga scala. Per ulteriori informazioni sull'implementazione di meccanismi di governance su larga scala, consulta AWS Governance at Scale. Dopo aver compreso in che modo la tua organizzazione ha organizzato e governato gli account AWS, considera i seguenti modelli di risposta generalizzati per identificare gli approcci giusti per l'organizzazione.

Argomenti



## Accesso indiretto

Se utilizzi l'accesso indiretto, i proprietari degli account o i team delle applicazioni sono tenuti a eseguire correzioni autorizzate nei loro account AWS con la guida tattica del team di risposta agli incidenti che sono i tuoi esperti di sicurezza. Questo metodo è un modo più lento e complesso per eseguire le attività, ma può avere successo quando i team di risposta non hanno familiarità con l'account o l'ambiente cloud.

## Accesso diretto

Per consentire l'accesso diretto agli incident responder, implementa un ruolo AWS IAM negli account AWS che i tuoi tecnici della sicurezza o i incident responder possono assumere durante un evento di sicurezza. L'incident responder esegue l'autenticazione tramite un normale processo federato o tramite uno speciale processo di emergenza, se l'incidente influisce sul normale processo di autenticazione. Le autorizzazioni assegnate al ruolo IAM di incident responder dipendono dalle operazioni che prevedi che i risponditori eseguano.

## Accesso alternativo

Se ritieni che un evento di sicurezza stia avendo un impatto sulla sicurezza, l'identità o i sistemi di comunicazione, potresti dover cercare meccanismi e accessi alternativi per indagare e rimediare all'impatto. Utilizzando un nuovo account AWS appositamente creato, i risponditori possono collaborare e lavorare da un'infrastruttura alternativa e sicura.

Ad esempio, i risponditori possono sfruttare la nuova infrastruttura lanciata nel cloud, come le workstation remote che utilizzano Amazon WorkSpaces e i servizi e-mail forniti da Amazon WorkMail. Devi preparare controlli di accesso appropriati (utilizzando le policy IAM) per delegare l'accesso in modo che il tuo account AWS alternativo e sicuro possa assumere le autorizzazioni per l'account AWS interessato.

Dopo aver delegato l'accesso appropriato, puoi utilizzare le API AWS nell'account interessato per condividere dati rilevanti, come i registri e gli snapshot di volumi, per eseguire attività investigative nell'ambiente isolato. Per ulteriori informazioni su questo accesso tra account, consulta Tutorial: Delega dell'accesso tra account AWS tramite i ruoli IAM.

## Accesso all'automazione

Quando esegui la migrazione all'utilizzo dell'automazione per rispondere agli eventi di sicurezza, devi creare ruoli IAM specifici per le risorse di automazione da utilizzare (ad esempio istanze Amazon EC2 o funzioni AWS Lambda). Queste risorse possono quindi assumere i ruoli IAM ed ereditare le autorizzazioni assegnate al ruolo. Invece di creare e distribuire credenziali AWS, deleghi l'autorizzazione alla funzione AWS Lambda o istanza Amazon EC2. La risorsa AWS riceve automaticamente una serie di credenziali temporanee e le utilizza per firmare le richieste API.

Puoi anche considerare un metodo sicuro per l'automazione o gli strumenti per l'autenticazione e l'esecuzione all'interno del sistema operativo dell'istanza Amazon EC2. Sebbene ci siano molti strumenti in grado di eseguire questa automazione, considera l'utilizzo di Run Command di AWS Systems Manager, che consente di amministrare in remoto e in modo sicuro le istanze utilizzando un agente installato sul sistema operativo dell'istanza Amazon EC2.

AWS Systems Manager Agent (SSM Agent) viene installato di default su alcune Amazon Machine Image (AMI) di Amazon EC2, ad esempio per Microsoft Windows Server e Amazon Linux. Tuttavia, potrebbe essere necessario installare manualmente l'agente su altre versioni di istanze Linux e istanze ibride. Sia che si utilizzi Run Command o un altro strumento, completare l'installazione e la configurazione dei prerequisiti prima di ricevere il primo avviso relativo alla sicurezza da esaminare.

## Accesso ai servizi gestiti

L'organizzazione potrebbe già essere partner di un fornitore di servizi informatici che gestisce servizi e soluzioni per tuo conto. Questi partner hanno una responsabilità condivisa nel supportare la sicurezza dell'organizzazione ed è importante comprendere chiaramente questa relazione prima che si verifichi un'anomalia. Sia che tu collabori già con un partner fornitore di servizi gestiti AWS (MSP), o AWS Managed Services oppure con un partner di servizi di sicurezza gestiti, devi identificare le responsabilità di ciascun partner in relazione ai tuoi ambienti cloud, di che tipo di accesso ai servizi cloud dispongono già i fornitori, dell'accesso di cui hanno bisogno e dei punti di contatto o dei percorsi di escalation per quando è richiesta la loro assistenza. Infine, dovresti esercitarti con il partner per assicurarti che i tuoi piani di risposta siano prevedibili e corretti.

# Preparazione dei processi

Una volta effettuato il provisioning e il test dell'accesso appropriato, il team di risposta agli incidenti deve definire e preparare i processi correlati necessari per l'indagine e la risoluzione dei problemi. Questa fase richiede molto impegno perché è necessario pianificare in modo sufficiente la risposta appropriata agli eventi di sicurezza all'interno degli ambienti cloud.

Collabora a stretto contatto con i team e i partner dei servizi cloud interni per identificare le attività necessarie per garantire che questi processi siano possibili. Collaborare o assegnarsi reciprocamente le attività di risposta e assicurarsi che siano disponibili le necessarie configurazioni dell'account. Consigliamo di preparare in anticipo i processi e le configurazioni dei prerequisiti per fornire all'organizzazione le seguenti capacità di risposta.

Argomenti

## Strutture decisionali

A volte, condizioni diverse possono richiedere operazioni o passaggi diversi. Ad esempio, le operazioni da effettuare potrebbero essere diverse in base al tipo di account AWS (sviluppo rispetto a produzione), ai tag delle risorse, allo stato di conformità alle regole AWS Config di tali risorse o ad altri input.

Per un supporto per la creazione e la documentazione relativa a queste decisioni, consigliamo di redigere un albero decisionale con gli altri team e le parti interessate. Simile a un diagramma di flusso, un albero decisionale è uno strumento che può essere sfruttato per supportare il processo decisionale, aiutando a determinare le operazioni e i risultati ottimali in base a potenziali condizioni e input, comprese le probabilità.

## Utilizzo di account alternativi

Sebbene possa essere necessario rispondere a un evento nell'account interessato, è l'ideale per esaminare i dati al di fuori dell'account interessato. Alcuni clienti dispongono di un processo per creare ambienti di account AWS separati e isolati, utilizzando modelli che preconfigurano le risorse di cui devono effettuare il provisioning. Questi modelli vengono implementati tramite un servizio, ad esempio AWS CloudFormation o Terraform, che fornisce un metodo semplice per creare una raccolta di risorse AWS correlate e per effettuarne il provisioning in modo ordinato e prevedibile.

La preconfigurazione di questi account utilizzando meccanismi basati su modelli aiuta a eliminare le interazioni umane durante le fasi iniziali di un incidente e garantisce che l'ambiente e le risorse siano preparati in modo ripetibile e prevedibile e tali operazioni possono essere sottoposte a verifica. Inoltre, questo meccanismo aumenta anche la capacità di mantenere la sicurezza e il contenimento dei dati nell'ambiente forense.

Questo approccio richiede di collaborare con i servizi cloud e i team di architetti per determinare un processo di account AWS appropriato che possa essere utilizzato per le indagini. Ad esempio, i team dei servizi cloud potrebbero utilizzare AWS Organizations per generare nuovi account e assistere l'utente nella preconfigurazione di tali account utilizzando un metodo basato su modelli o script.

Questo metodo di segmentazione è ideale quando è necessario mantenere un'organizzazione più grande lontana da una potenziale minaccia. Questa segmentazione, mediante l'utilizzo di un account AWS nuovo e principalmente non connesso, consente a un utente dell'organizzazione, etichettato nella documentazione multi-account come unità organizzativa (UO) di sicurezza, di spostarsi nell'account, eseguire le attività forensi necessarie e potenzialmente trasferire l'account nel suo insieme a un'entità giuridica, se necessario. Questo metodo di analisi forense e di

attribuzione richiede un'esame e una pianificazione significative e dovrebbe allinearsi alle policy GRC dell'azienda. Sebbene questa operazione non sia semplice, è molto più facile effettuarla prima di creare un'ampia base di account.

## Visualizzazione o copia dei dati

I risponditori richiedono l'accesso ai registri o ad altre prove per l'analisi e devono assicurarsi di avere la capacità di visualizzare o copiare i dati. Come minimo, la policy di autorizzazione IAM per i risponditori dovrebbe fornire un accesso di sola lettura in modo che possano indagare. Per abilitare l'accesso appropriato, è possibile considerare alcune policy predefinite gestite da AWS, come SecurityAudit o ViewOnlyAccess.

Ad esempio, i risponditori potrebbero voler creare una copia point-in-time dei dati, come i registri AWS CloudTrail, da un bucket Simple Storage Service (Amazon S3) in un account a un bucket Simple Storage Service (Amazon S3) in un altro account. Le autorizzazioni fornite dalla policy gestita ReadOnlyAccess, ad esempio, consentono al risponditore di eseguire queste operazioni. Per informazioni su come utilizzare l'Interfaccia a riga di comando AWS (CLI) per eseguire questa operazione, consulta Come è possibile copiare tutti gli oggetti da un bucket Simple Storage Service (Amazon S3) a un altro?.

## Condivisione di snapshot di Amazon EBS

Molti clienti utilizzano gli snapshot di Amazon Elastic Block Store (Amazon EBS) come parte della loro indagine per eventi di sicurezza che coinvolgono le istanze Amazon EC2. Gli snapshot dei volumi Amazon EBS sono backup incrementali. Per ulteriori informazioni sugli snapshot incrementali di Amazon EBS, consulta Snapshot di Amazon EBS.

Per eseguire un'indagine su un volume Amazon EBS in un account separato e isolato, è necessario modificare le autorizzazioni dello snapshot per condividerlo con gli altri account AWS specificati. Gli utenti autorizzati possono utilizzare lo snapshot condiviso come base per la creazione di propri volumi EBS, mentre lo snapshot originale rimane inalterato. Per ulteriori informazioni, consulta Condivisione di uno snapshot Amazon EBS.

Se lo snapshot è crittografato, è necessario condividere anche la chiave personalizzata AWS Key Management Service (AWS KMS) gestita dal cliente (CMK) utilizzata per crittografare lo snapshot. È possibile applicare autorizzazioni valide su più account a una chiave CMK personalizzata al momento della creazione o in un secondo momento. Gli snapshot sono vincolati alla regione in cui sono stati creati, ma è possibile condividere uno snapshot con un'altra regione copiando lo snapshot in quella regione. Per ulteriori informazioni, consulta Copia di uno snapshot Amazon EBS.

## Condivisione di Amazon CloudWatch Logs

I registri registrati in Amazon CloudWatch Logs, come i flussi di log Amazon VPC, possono essere condivisi con un altro account (ad esempio l'account di sicurezza centralizzato) tramite un abbonamento a CloudWatch Logs. Ad esempio, questi dati di eventi di registro possono essere letti da un flusso di Amazon Kinesis centralizzato per eseguire elaborazioni e analisi personalizzate. L'elaborazione personalizzata è particolarmente utile quando si raccolgono dati di registrazione da molti account. Idealmente, crea questa configurazione all'inizio del percorso verso il cloud, prima che si verifichi un evento relativo alla sicurezza. Per ulteriori informazioni, consulta Condivisione di dati di registro tra più account con le sottoscrizioni.

## Utilizzo dell'archiviazione immutabile

Quando si copiano registri e altre prove su un account alternativo, assicurarsi che i dati replicati siano protetti. Oltre a proteggere le prove secondarie, è necessario proteggere anche l'integrità dei dati alla fonte. Conosciuti come archiviazione immutabile, questi meccanismi proteggono l'integrità dei dati impedendo che vengano manomessi o eliminati.

Utilizzando le caratteristiche native di Amazon S3, puoi configurare un bucket Simple Storage Service (Amazon S3) per proteggere l'integrità dei dati. Utilizzando il blocco oggetti S3, puoi impedire che un oggetto venga eliminato o sovrascritto per un determinato periodo di tempo o in modo indefinito. La gestione delle autorizzazioni di accesso con le policy dei bucket S3, la configurazione del controllo delle versioni S3 e l'abilitazione dell'eliminazione di MFA sono altri modi per limitare la scrittura o la lettura dei dati. Questo tipo di configurazione è utile per archiviare i registri e le prove delle indagini e viene spesso definita come WORM (write once, read many). È inoltre possibile proteggere i dati utilizzando la crittografia lato server con AWS Key Management Service (AWS KMS) e verificando che solo i principali IAM appropriati siano autorizzati a decrittare i dati.

Inoltre, se desideri conservare in modo sicuro i dati in un'archiviazione a lungo termine dopo il completamento dell'indagine, valuta la possibilità di spostare i dati da Simple Storage Service (Amazon S3) ad Amazon S3 Glacier utilizzando le policy del ciclo di vita degli oggetti. Amazon S3 Glacier è un servizio di archiviazione nel cloud sicuro, duraturo ed estremamente economico per l'archiviazione dei dati e il backup a lungo termine. È progettato per offrire una durabilità del 99,999999999% e offre funzionalità complete di sicurezza e conformità.

Inoltre, puoi proteggere i dati in Amazon S3 Glacier utilizzando Amazon S3 Glacier Vault Lock, che consente di implementare e applicare facilmente i controlli di conformità per i singoli vault di Amazon S3 Glacier con una policy di Vault Lock. Puoi specificare controlli di sicurezza di tipo WORM (Write

Once Read Many) in una policy di Vault Lock e bloccare la policy per impedire modifiche future. Una volta bloccata, la policy non può essere modificata. Amazon S3 Glacier applica i controlli impostati nella policy di Vault Lock per consentirti di raggiungere gli obiettivi di conformità, come ad esempio la conservazione dei dati. È possibile implementare una serie di controlli di conformità in una policy di Vault Lock utilizzando il linguaggio delle policy AWS Identity and Access Management (IAM).

## Avvio delle risorse in prossimità dell'evento

Per i risponditori che non conoscono il cloud, si può avere la tentazione di condurre indagini sul cloud in locale dove si trovano gli strumenti esistenti. In base alla nostra esperienza, i clienti AWS che rispondono agli incidenti utilizzando tecnologie cloud ottengono risultati migliori: gli isolamenti possono essere automatizzati, le copie possono essere create più facilmente, le prove sono pronte per l'analisi prima e l'analisi può essere completata più velocemente.

La best practice è quella di eseguire indagini e indagini forensi nel cloud, dove si trovano i dati, piuttosto che tentare di trasferire i dati a un data center prima di indagare. È possibile utilizzare le funzionalità di calcolo e archiviazione sicuri del cloud praticamente in qualsiasi parte del mondo per eseguire le operazioni di risposta sicura. Molti clienti scelgono di creare in anticipo un account AWS separato pronto per eseguire un'indagine, anche se potrebbero esserci casi in cui si sceglie di eseguire l'analisi nello stesso account AWS. Se si prevede che l'organizzazione conservi i registri per motivi legali e di conformità, potrebbe essere prudente mantenere account separati per l'archiviazione a lungo termine e le attività legali.

È inoltre consigliabile eseguire l'indagine nella stessa regione AWS in cui si è verificato l'evento, piuttosto che replicare i dati in un'altra regione. Consigliamo questa pratica principalmente a causa del tempo aggiuntivo necessario per trasferire i dati tra le regioni. Per ogni regione AWS in cui operi, assicurati che sia il tuo processo di risposta agli incidenti e che i risponditori rispettino le leggi sulla privacy dei dati pertinenti. Se hai bisogno di spostare dati tra regioni, considera le implicazioni legali dello spostamento di dati tra giurisdizioni. È generalmente una best practice conservare i dati all'interno della stessa giurisdizione nazionale.

Se ritieni che un evento di sicurezza stia avendo un impatto sulla sicurezza, l'identità o i sistemi di comunicazione, potresti dover cercare meccanismi e accessi alternativi per indagare e rimediare all'impatto. AWS ti offre la possibilità di avviare rapidamente una nuova infrastruttura che può essere utilizzata per ambienti di lavoro alternativi e sicuri. Ad esempio, durante l'indagine sulla potenziale gravità della situazione, potresti voler creare un nuovo account AWS con gli strumenti sicuri necessari al tuo consulente legale, alle pubbliche relazioni e ai team di sicurezza per comunicare e continuare a lavorare. Servizi come AWS WorkSpaces (per desktop virtuali), AWS WorkMail (per e-mail) e

Amazon Chime (per le comunicazioni) possono fornire ai team di risposta, ai dirigenti e agli altri partecipanti le funzionalità e la connettività necessarie per comunicare, indagare e risolvere un problema.

## Isolamento delle risorse

Nel corso dell'indagine, potrebbe essere necessario isolare le risorse come parte della risposta a un'anomalia di sicurezza. L'obiettivo alla base dell'isolamento delle risorse è limitare il potenziale impatto, prevenire un'ulteriore propagazione delle risorse interessate, limitare l'esposizione involontaria dei dati e impedire ulteriori accessi non autorizzati.

Come per qualsiasi risposta, possono essere applicate considerazioni aziendali, normative, legali o di altro tipo. Assicurati di valutare le operazioni pianificate rispetto alle conseguenze previste e impreviste. Se i team del cloud utilizzano tag delle risorse, questi tag possono aiutarti a identificare la criticità della risorsa o del proprietario da contattare.

## Avvio delle workstation forensi

Alcune delle attività di risposta agli incidenti potrebbero includere l'analisi di immagini del disco, file system, dump della RAM o altri artefatti coinvolti in un incidente. Molti clienti creano una workstation forense personalizzata che possono utilizzare per montare copie di qualsiasi volume di dati interessato (noti come snapshot EBS). Per fare ciò, segui i passaggi di base indicati di seguito:

1. Scegli un'Amazon Machine Image (AMI) di base (come Linux o Microsoft Windows) che può essere utilizzata come workstation forense.
2. Avvia un'istanza Amazon EC2 dall'AMI di base.
3. Rafforza il sistema operativo, rimuovi i pacchetti software non necessari e configura i meccanismi di verifica e registrazione pertinenti.
4. Installa la suite preferita di kit di strumenti open source o privati, nonché qualsiasi software e pacchetto del fornitore di cui hai bisogno.
5. Arresta l'istanza Amazon EC2 e crea una nuova AMI dall'istanza arrestata.
6. Crea un processo settimanale o mensile per aggiornare e ricostruire l'AMI con le patch software più recenti.

Dopo aver effettuato il provisioning del sistema forense tramite un'AMI, il team di risposta agli incidenti può utilizzare questo modello per creare una nuova AMI per avviare una nuova workstation

forense per ogni indagine. Il processo di avvio dell'AMI come istanza Amazon EC2 può essere preconfigurato per semplificare il processo di implementazione. Ad esempio, puoi creare un modello delle risorse dell'infrastruttura forense di cui hai bisogno in un file di testo e implementarli nell'account AWS utilizzando AWS CloudFormation.

Quando le risorse sono disponibili per essere implementate rapidamente da un modello, gli esperti forensi ben addestrati sono in grado di utilizzare nuove workstation forensi per ogni indagine, invece di riutilizzare l'infrastruttura. Con questo processo, è possibile assicurarsi che non vi siano contaminazioni incrociate da altri esami forensi.

### Tipi e posizioni delle istanze

Amazon EC2 offre un'ampia gamma di tipi di istanze ottimizzati per soddisfare diversi casi d'uso. I tipi di istanze comprendono diverse combinazioni di capacità di CPU, memoria, archiviazione e di rete, offrendo la flessibilità di poter scegliere la combinazione di risorse adeguata per le proprie applicazioni. Molti tipi di istanze includono più dimensioni di istanze, che consentono di dimensionare le risorse in base ai requisiti del carico di lavoro di destinazione. Per le istanze di risposta agli incidenti, seguire le policy GRC dell'azienda per la posizione e la segmentazione dalla rete che esegue le istanze di produzione.

Le reti avanzate AWS utilizzano la specifica SR-IOV (Single Root I/O Virtualization) per fornire funzionalità di rete a prestazioni elevate sui tipi di istanza supportati. SR-IOV è un metodo di virtualizzazione dei dispositivi che fornisce prestazioni I/O più elevate e minore utilizzo della CPU rispetto alle interfacce di rete virtualizzate tradizionali. Le reti avanzate forniscono infatti una larghezza di banda più alta, prestazioni PPS (pacchetti al secondo) superiori e latenze tra istanze significativamente più basse. L'utilizzo di questo servizio avanzato non comporta costi supplementari. Per informazioni sui tipi di istanza che supportano velocità di rete a 10 o 25 Gbps e altre funzionalità avanzate, consulta Tipi di istanze Amazon EC2.

## Supporto del fornitore di servizi cloud

Argomenti

- AWS Managed Services
- AWS Support
- Supporto DDoS Response

## AWS Managed Services

AWS Managed Services (AMS) offre la gestione continua dell'infrastruttura AWS permettendo ai clienti di occuparsi a tempo pieno delle proprie applicazioni. Implementando le best practice per la manutenzione dell'infrastruttura, AMS consente di ridurre i rischi e i costi operativi. AMS automatizza attività frequenti quali richieste di modifica, monitoraggio, gestione di patch, sicurezza e servizi di backup, nonché fornisce servizi completi per il ciclo di vita per gestire provisioning, esecuzione e supporto dell'infrastruttura.

In qualità di operatore dell'infrastruttura, AMS si assume la responsabilità di implementare una serie di controlli di rilevazione di sicurezza e fornisce una prima linea di risposta agli avvisi 24 ore su 24, 7 giorni su 7, utilizzando un modello "follow-the-sun". Quando viene attivato un avviso, AMS segue un set standard di runbook automatici e manuali per garantire una risposta coerente. Questi runbook vengono condivisi con i clienti AMS durante l'onboarding in modo che possano sviluppare e coordinare la risposta con AMS. AMS incoraggia l'esecuzione congiunta di simulazioni di risposta alla sicurezza con i clienti per sviluppare la capacità operativa prima che si verifichi un incidente reale.

## AWS Support

AWS Support offre un'ampia gamma di piani che forniscono l'accesso agli strumenti e alle competenze che contribuiscono al successo e all'integrità operativa delle soluzioni AWS. Tutti i piani di supporto forniscono accesso 24 ore su 24, 7 giorni su 7 al servizio clienti, alla documentazione di AWS, ai whitepaper e ai forum di supporto. Se ti occorrono supporto tecnico e risorse aggiuntive che aiutano a pianificare, implementare e ottimizzare l'ambiente AWS, puoi scegliere il piano di supporto che più si allinea al tuo caso d'uso di AWS.

Dovresti considerare il Support Center nella AWS Management Console come il punto di contatto centrale per ottenere supporto per problemi che riguardano le risorse AWS. L'accesso a AWS Support è controllato da IAM. Per ulteriori informazioni su come ottenere l'accesso alle caratteristiche di supporto di AWS, consulta Accesso al supporto.

Inoltre, se devi segnalare un uso illecito di Amazon EC2, contatta il team di AWS che si occupa degli usi illeciti.

## Supporto DDoS Response

Un attacco Denial of Service (DoS) rende il tuo sito Web o la tua applicazione non disponibile per gli utenti finali. Gli aggressori utilizzano una varietà di tecniche che consumano la larghezza di banda della rete o altre risorse, interrompendo l'accesso per gli utenti finali legittimi. Nella sua forma più

semplice, un attacco DoS contro un bersaglio viene eseguito da un utente malintenzionato solitario da un'unica fonte.

In un attacco DDoS (Distributed Denial of Service), un utente malintenzionato utilizza più fonti, che possono essere compromesse o controllate da un gruppo di collaboratori, per orchestrare un attacco contro un bersaglio. In un attacco DDoS, ogni collaboratore o host compromesso partecipa all'attacco, generando un flusso di pacchetti o richieste per sovraccaricare il bersaglio previsto.

AWS offre ai clienti AWS Shield che è un servizio di protezione DDoS (Distributed Denial of Service) gestito che protegge le applicazioni Web in esecuzione su AWS. AWS Shield fornisce un rilevamento sempre attivo e mitigazioni automatiche in linea che riducono al minimo i tempi di inattività e la latenza delle applicazioni, quindi non è necessario coinvolgere AWS Support per beneficiare della protezione DDoS. Sono disponibili due livelli di AWS Shield: Standard e Avanzato.

Tutti i clienti AWS beneficiano della protezione automatica di AWS Shield Standard, senza costi aggiuntivi. AWS Shield Standard protegge dagli attacchi DDoS a livello di rete e di trasporto più comuni e frequenti a siti Web o applicazioni. Chi utilizza AWS Shield Standard con Amazon CloudFront e Amazon Route 53, potrà avvalersi della protezione completa contro tutti gli attacchi a livello di infrastruttura (livello 3 e 4).

Per livelli di protezione più elevati contro gli attacchi diretti alle applicazioni Web su risorse di Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB), Amazon CloudFront e Amazon Route 53, è possibile eseguire la registrazione ad AWS Shield Advanced. Inoltre, AWS Shield Advanced offre accesso 24 ore su 24, 7 giorni su 7 al team di risposta DDoS (DRT) di AWS. Per ulteriori informazioni su AWS Shield Standard e AWS Shield Advanced, consulta AWS Shield.

# Simulazione

Argomenti



## Simulazioni di risposta agli incidenti di sicurezza

Le simulazioni di risposta agli incidenti di sicurezza (SIRS) sono eventi interni che forniscono un'opportunità strutturata per mettere in pratica il piano e le procedure di risposta agli incidenti in uno scenario realistico. Gli eventi SIRS riguardano fondamentalmente la preparazione e il miglioramento iterativo delle capacità di risposta. Alcuni dei motivi per cui i clienti trovano valore nello svolgimento delle attività SIRS includono:

- Convalida della preparazione.
- Sviluppo delle competenze mediante l'apprendimento da simulazioni e dal personale preposto alla formazione.
- Rispetto degli obblighi contrattuali o di conformità.
- Generazione di artefatti per l'accreditamento.
- Essere agili e ottenere miglioramenti incrementali con attenzione.
- Miglioramento della velocità e degli strumenti.
- Perfezionamento della comunicazione e dell'escalation.
- Gestione più sicura delle situazioni rare e impreviste.

Per questi motivi, il valore derivato dalla partecipazione a un'attività SIRS (Security Incident Response Simulation) aumenta l'efficacia di un'organizzazione durante gli eventi stressanti. Sviluppare un'attività SIRS realistica e utile può essere un esercizio difficile. Anche se testare le procedure o l'automazione che gestisce eventi noti presenta alcuni vantaggi, è altrettanto utile partecipare alle attività SIRS creative per mettersi alla prova in situazioni impreviste.

# Fasi di simulazione

Indipendentemente dal fatto che tu stia progettando il tuo SIRS o che tu abbia un partner fidato per fornire le basi, le simulazioni generalmente seguono questi passaggi:

1. Trovare un problema importante: definisci l'attivazione che dovrebbe causare una risposta.
2. Identificare tecnici specializzati nella sicurezza: una simulazione richiede un costruttore e un tester.
3. Costruire un sistema di modelli realistico: la simulazione deve essere realistica e appropriata. Se non è realistica, i partecipanti potrebbero non ricavare valore dall'esercizio. Se è troppo essenziale, l'esercizio potrebbe essere considerato banale. Iniziare con semplici esercizi e lavorare per un evento completo.
4. Creazione e test degli elementi dello scenario: potrebbe essere necessario creare materiale di simulazione pertinente, come artefatti di registrazione, notifiche e avvisi e-mail e potenziali runbook.
5. Invita altri addetti alla sicurezza e partecipanti tra le organizzazioni:  invita tutti coloro che devono formarsi e partecipare. Se il tuo consulente legale generale, i dirigenti e le pubbliche relazioni hanno un ruolo nella simulazione, dovresti invitare anche loro.
6. Eseguire la simulazione: scegli se il personale deve aspettarsi l'evento SIRS o se la simulazione deve avvenire senza preavviso.
7. Celebrare, misurare, migliorare e ripetere: la simulazione ha fattori di stress, quindi è importante incoraggiare e premiare gli sforzi dei partecipanti. Dopo l'incoraggiamento arriva l'opportunità di misurare, migliorare e ripetere per la prossima simulazione. AWS incoraggia a rendere abituali queste attività.

> **Important**
>
> Se si sta pianificando una Security Incident Response Simulation (SIRS), consulta Test di penetrazione (pen-test) ed esamina la sezione Altri eventi simulati per le informazioni più aggiornate su come procedere.

# Esempi di simulazione

Le simulazioni di sicurezza devono essere realistiche affinché abbiano valore. Quando tu o i tuoi partner lavorate per creare le simulazioni, considera sempre gli eventi reali che sono avvenuti come

una fonte preziosa per potenziali esercizi di simulazione. Ecco alcuni esempi che i clienti AWS hanno trovato utile utilizzare per le loro simulazioni iniziali:

- Modifiche non autorizzate alla configurazione o alle risorse di rete.
- Credenziali che sono state erroneamente esposte pubblicamente a causa di errori di configurazione dello sviluppatore.
- Contenuti sensibili che sono stati erroneamente resi pubblicamente accessibili a causa di un'errata configurazione dello sviluppatore.
- Isolamento di un server Web che comunica con indirizzi IP sospetti dannosi.

Oltre al prezioso apprendimento grazie all'esperienza, l'esecuzione di attività SIRS genera risultati, come le lezioni apprese, che è possibile utilizzare come input nel prossimo processo del programma: l'iterazione.

# Iterare

La sezione precedente ha definito alcuni dei vantaggi delle attività SIRS. Tra questi vantaggi c'era l'aumento dell'agilità (metodologia agile) attraverso miglioramenti incrementali. Le simulazioni dovrebbero generare risultati preziosi che è possibile sfruttare per migliorare la risposta alla sicurezza. Forniscono un circuito di feedback all'organizzazione, su cosa funziona e cosa non funziona. Con queste conoscenze, puoi creare in modo incrementale nuove procedure o aggiornare quelle esistenti per migliorare la risposta.

Argomenti



## Runbook

Quando viene rilevata un'anomalia di sicurezza, il contenimento dell'evento e il ritorno a uno stato valido sono elementi importanti di un piano di risposta. Ad esempio, se l'anomalia si è verificata a causa di un'errata configurazione della sicurezza, la correzione potrebbe essere semplice come rimuovere la varianza attraverso una ridistribuzione delle risorse con la configurazione corretta. Per fare ciò, dovrai pianificare in anticipo e definire le procedure di risposta alla sicurezza, che sono spesso chiamate runbook.

Un runbook è la forma documentata delle procedure di un'organizzazione per lo svolgimento di un'attività o di una serie di attività. Questa documentazione viene di solito archiviata in un sistema digitale interno o su carta stampata. Al momento potresti avere runbook di risposta agli incidenti o potrebbe essere necessario crearli per essere conformi a un framework di garanzia della sicurezza. Tuttavia, quando segui manualmente i runbook scritti, aumenti la possibilità di commettere errori. Ti consigliamo invece di automatizzare tutte le attività ripetibili. L'automazione libera il team di risposta dalle attività comuni e lo rende disponibile per attività più importanti, come la correlazione di eventi, la pratica nelle simulazioni, l'elaborazione di nuove procedure di risposta, l'esecuzione di ricerche, lo sviluppo di nuove competenze e il test o la creazione di nuovi strumenti. Tuttavia, prima di poter scomporre le attività in logica programmabile e iterare verso una corretta automazione, è necessario iniziare scrivendo un runbook.

## Creazione di runbook

Per creare runbook per il cloud, ti consigliamo di concentrarti prima sugli avvisi che generi attualmente. Se si genera un avviso, è importante esaminarlo. Inizia definendo le descrizioni dei processi manuali che esegui. Successivamente, testa i processi ed esegui l'iterazione sul modello runbook per migliorare la logica di base della risposta. Determina quali sono le eccezioni e quali sono le risoluzioni alternative per tali scenari. Ad esempio, in un ambiente di sviluppo, potresti voler terminare un'istanza Amazon EC2 configurata in modo errato. Tuttavia, se lo stesso evento si è verificato in un ambiente di produzione, invece di terminare l'istanza puoi arrestare l'istanza e verificare con le parti interessate che i dati critici non vadano persi e che l'interruzione sia accettabile.

Dopo aver determinato la soluzione migliore, puoi scomporre la logica in una soluzione basata su codice, che può essere utilizzata come strumento da molti soccorritori per automatizzare la risposta e rimuovere la varianza o le congetture da parte del team di risposta. Questo accelera il ciclo di vita di una risposta. L'obiettivo successivo è abilitare questo codice in modo che sia completamente automatizzato e che possa essere richiamato dagli avvisi o dagli eventi stessi, piuttosto che da un addetto alle risposte, per creare una risposta basata sugli eventi.

## Nozioni di base

Se non sai da dove iniziare, considera di iniziare con gli avvisi che potrebbero essere generati da AWS Trusted Advisor, le best practice di sicurezza fondamentali di AWS Security Hub e Regole di AWS Config (tra cui ilrepository Github Regole di AWS Config). Quindi, concentrati sugli eventi generati dai servizi che descriveranno i sistemi che ti interessano.

Amazon GuardDuty e Access Analyzer descrivono molti degli ambiti che un'applicazione utilizzerà in AWS, motivo per cui sono generalmente suggeriti; tuttavia, Amazon Inspector e Amazon Macie hanno usi specifici per coloro che hanno problemi di dati e di endpoint. Le informazioni sui risultati di Amazon GuardDuty sono disponibili nella Guida per l'utente di Amazon GuardDuty. I risultati di Access Analyzer sono disponibili nella Guida per l'utente di Amazon Access Analyzer. I risultati di Macie sono disponibili nella Guida per l'utente di Amazon Macie. I risultati di Amazon Inspector sono disponibili nella Guida per l'utente di Amazon Inspector. Security Hub ti offre la possibilità di unificare tali risultati in un'unica posizione e reagire ad essi di concerto con una bassa latenza, motivo per cui viene suggerito come posizione centrale per la correzione.

Tutti i servizi descritti in precedenza inviano notifiche tramite Amazon CloudWatch Events ogni volta che si verificano modifiche nei risultati o negli avvisi, inclusi gli avvisi appena generati e gli aggiornamenti degli avvisi esistenti. È possibile impostare le regole di Amazon CloudWatch Events per attivare funzioni AWS Lambda per eseguire una risposta basata sugli eventi. Tuttavia, la

possibilità di creare informazioni dettagliate personalizzate e aggiungere i propri risultati dall'ambito dell'applicazione si aggiunge ai motivi importanti per utilizzare invece Security Hub. Per ulteriori informazioni, consulta la sezione Risposta basata sugli eventi.

# Automazione

L'automazione è un moltiplicatore di forza, il che significa che dimensiona gli sforzi dei team di risposta per adattarli alla velocità dell'organizzazione. Il passaggio da processi manuali a processi automatizzati consente di dedicare più tempo all'aumento della sicurezza dell'ambiente AWS Cloud.

Argomenti

- Automatizzazione della risposta agli incidenti
- Risposta basata sugli eventi

## Automatizzazione della risposta agli incidenti

Per automatizzare le funzioni delle operazioni e la progettazione della sicurezza, puoi utilizzare un set completo di API e strumenti di AWS. Puoi automatizzare completamente la gestione delle identità, la sicurezza della rete, la protezione dei dati e le funzionalità di monitoraggio. Quando crei l'automazione della sicurezza, il sistema può monitorare, rivedere e avviare una risposta, invece di far monitorare alle persone la posizione di sicurezza e reagire manualmente agli eventi.

Se i team di risposta agli incidenti continuano a rispondere agli avvisi nello stesso modo, rischiano il cosiddetto affaticamento dagli avvisi ("alert fatigue"). Ciò significa che, nel corso del tempo, il team può diventare desensibilizzato agli avvisi e può commettere errori nella gestione di situazioni ordinarie o farsi sfuggire avvisi insoliti. L'automazione aiuta a evitare l'affaticamento dagli avvisi utilizzando funzioni che elaborano gli avvisi ripetitivi e ordinari, lasciando alle persone la gestione degli incidenti sensibili e univoci.

Puoi migliorare i processi manuali automatizzando le fasi del processo a livello di programmazione. Dopo aver definito il modello di correzione di un evento, puoi scomporre tale modello in una logica fruibile e scrivere il codice per eseguire tale logica. Il team di risposta può quindi eseguire il codice per risolvere il problema. Nel corso del tempo, puoi automatizzare più fasi e, infine, gestire automaticamente intere classi di incidenti comuni.

Tuttavia, il tuo obiettivo dovrebbe essere quello di ridurre ulteriormente il divario temporale tra i meccanismi di rilevazione e i meccanismi reattivi. Storicamente, questo intervallo di tempo può richiedere ore, giorni o addirittura mesi. Un sondaggio sulla risposta agli incidenti condotto da

SANS nel 2016 ha rilevato che il 21% degli intervistati ha dichiarato che il tempo necessario per il rilevamento richiedeva da due a sette giorni e solo il 29% degli intervistati era in grado di rimediare agli eventi nello stesso lasso di tempo. Nel cloud, puoi ridurre tale intervallo di tempo di risposta a pochi secondi sviluppando funzionalità di risposta guidate dagli eventi.

Argomenti



## Opzioni per l'automazione della risposta

È importante assicurarsi di bilanciare l'implementazione aziendale e la struttura organizzativa. La Figura 4 illustra le differenze negli attributi tecnici per ciascuna opzione di risposta automatica nell'implementazione AWS con un grafico radar. Nel grafico, più l'attributo tecnico si sposta dal centro del grafico, maggiore è la forza di tale attributo tecnico per la risposta di automazione corrispondente. Ad esempio, AWS Lambda offre maggiore velocità e richiede meno competenze tecniche. AWS Fargate offre maggiore flessibilità e richiede meno manutenzione e competenze tecniche. La Tabella 1 fornisce una panoramica di queste opzioni di automazione e un riepilogo degli attributi tecnici di ciascuna.

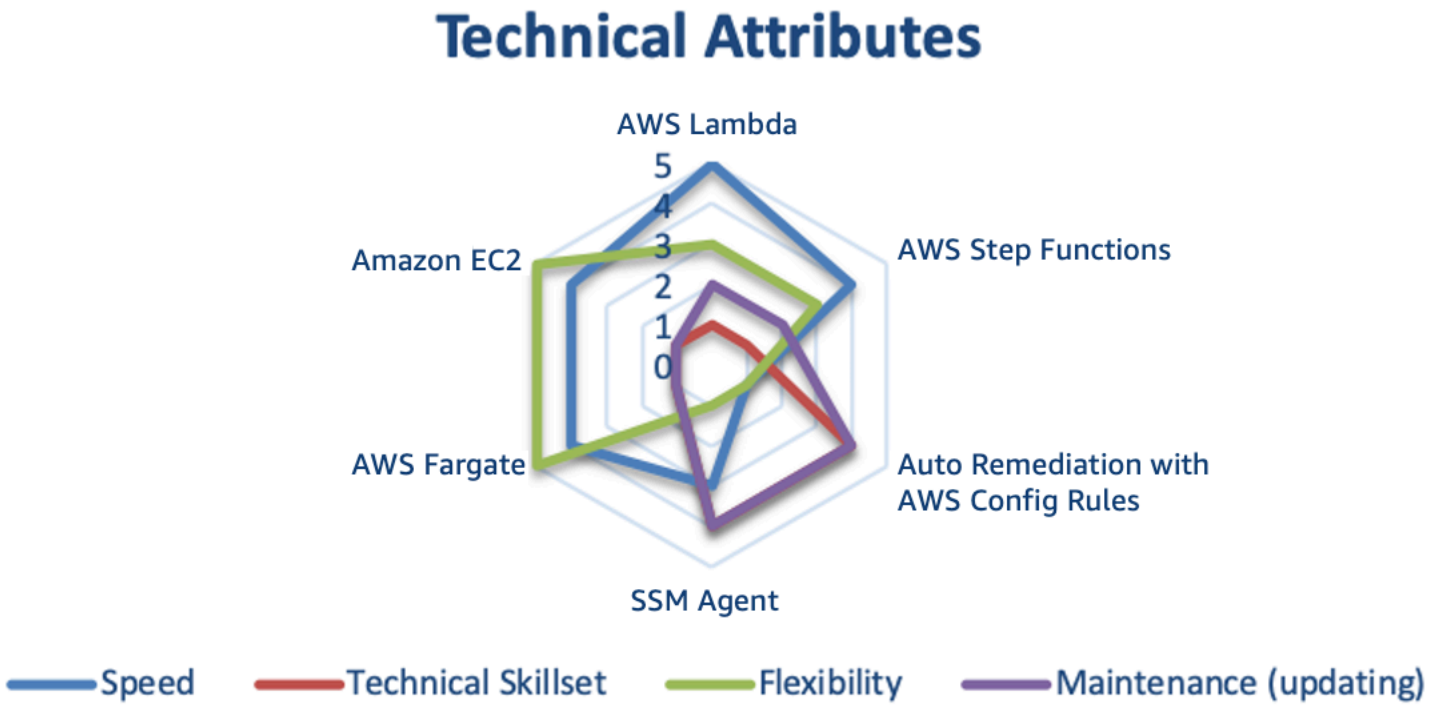


Figura 4: Differenze negli attributi tecnici tra gli approcci di risposta automatizzata

Tabella 1: Opzioni per la risposta automatica

| Servizio o caratteristica AWS | Descrizione | Riepilogo degli attributi* |
|---|---|---|
| AWS Lambda | Sistema che utilizza solo AWS Lambda, utilizzando il linguaggio aziendale dell'organizzazione. | Velocità<br>Flessibilità<br>Manutenzione<br>Competenze |
| AWS Step Functions | Sistema che utilizza AWS Step Functions, Lambda e l'SSM Agent. | Velocità<br>Flessibilità<br>Manutenzione<br>Competenze |
| Correzione automatica con Regole di AWS Config | Set di Regole di AWS Config e correzioni automatiche che valutano l'ambiente e lo reinseriscono nelle specifiche approvate. | Manutenzione e competenze<br>Velocità e flessibilità |
| SSM Agent | Insieme di regole e documenti di automazione che esaminano molti elementi degli ambienti e dei sistemi interni e apportano correzioni. | Manutenzione e competenze<br>Velocità<br>Flessibilità |
| AWS Fargate | Sistema AWS Fargate che utilizza il codice step function open source e gli eventi di Amazon CloudWatch e di altri sistemi per guidare il rilevamento e la correzione. | Flessibilità<br>Velocità<br>Manutenzione e competenze |

| Servizio o caratteristica AWS | Descrizione | Riepilogo degli attributi* |
|---|---|---|
| Amazon EC2 | Un sistema in esecuzione su un'istanza completa, simile all'opzione AWS Fargate. | Flessibilità<br>Velocità<br>Manutenzione<br>Competenze |

* Gli attributi sono elencati in ordine decrescente per ogni servizio o caratteristica. Ad esempio, AWS Lambda offre più velocità e richiede meno competenze tecniche. AWS Fargate offre maggiore flessibilità e richiede meno competenze tecniche e di manutenzione.

Quando consideri queste opzioni di automazione nell'ambiente AWS, devi anche considerare la centralizzazione e il periodo di scansione (eventi al secondo [EPS]).

Centralizzazione si riferisce a un account centrale che guida tutto il rilevamento e la correzione per un'organizzazione. Questo approccio può sembrare la scelta migliore ed è la best practice attuale. Tuttavia, alcune circostanze richiedono di deviare da questo approccio e capire quando dipende dalla gestione degli account subordinati. Ti invitiamo a iniziare sfruttando l'approccio dell'account Strumenti di sicurezza nel framework multi-account in AWS Organizations o AWS Control Tower.

Tabella 2: vantaggi e svantaggi della centralizzazione

| | Centralizzazione | Decentralizzazione |
|---|---|---|
| Vantaggi | Gestione della configurazione semplice<br>Impossibile annullare o modificare la risposta | Architettura semplice<br>Configurazione iniziale più rapida |
| Svantaggi | Maggiore complessità nell'architettura<br>Account e risorse di onboarding/revoca dell'accesso | Ulteriori risorse da gestire<br>Difficoltà a mantenere una linea di base del software |

Un confronto dei costi per queste implementazioni può anche guidare la decisione aziendale nel determinare l'opzione migliore. Events al secondo (EPS) è il parametro utilizzato per stimare al meglio i costi. Potrebbe, alla fine, essere molto più facile ed economico utilizzare approcci centralizzati o decentralizzati, ma è impossibile per noi esaminare come valuterai quel costo specificamente nel tuo account. Assicurati di considerare l'EPS quando invii questi eventi a un account centrale per ricevere una risposta. Maggiore è il numero di EPS, maggiore è il costo di invio di tali eventi a un account centralizzato.

## Confronti dei costi nei metodi di scansione

I costi sono ulteriormente determinati dal metodo di scansione con cui viene rilevata un'anomalia e dall'intervallo di tempo tra le convalide. Per i metodi di scansione, è possibile scegliere tra l'esame della scansione basata su eventi o della scansione periodica. La tabella 3 mostra i vantaggi e svantaggi di entrambi gli approcci.

Tabella 3: Vantaggi e svantaggi dei diversi metodi di scansione

| | Basata su eventi | Scansione periodica |
|---|---|---|
| Vantaggi | Meno tempo dall'evento alla risposta<br><br>Necessità limitata di eseguire query su chiamate API aggiuntive | Immagine completa in un determinato momento |
| Svantaggi | Contesto limitato dello stato della risorsa<br><br>Gli eventi attivati possono riguardare una risorsa non immediatamente disponibile | Limiti del servizio nei confronti di account di grandi dimension i<br><br>Può potenzialmente incorrere nella limitazione (della larghezza della banda di rete) a causa dell'elevato volume di chiamate API |

In molti casi, una combinazione di entrambi gli approcci di scansione è probabilmente la scelta migliore in un'organizzazione consolidata. AWS Security Hub e lo Standard AWS Foundational Security Best Practices fornisce una combinazione di entrambi i metodi di scansione.

La Figura 5 fornisce un grafico radar che illustra il confronto dei costi degli eventi al secondo (EPS) per ciascuno degli approcci di automazione. Ad esempio, Amazon EC2 e AWS Fargate hanno i costi più elevati per l'esecuzione di 0-10 EPS, mentre AWS Lambda e AWS Step Functions hanno i costi più elevati per l'esecuzione di oltre 76 EPS.

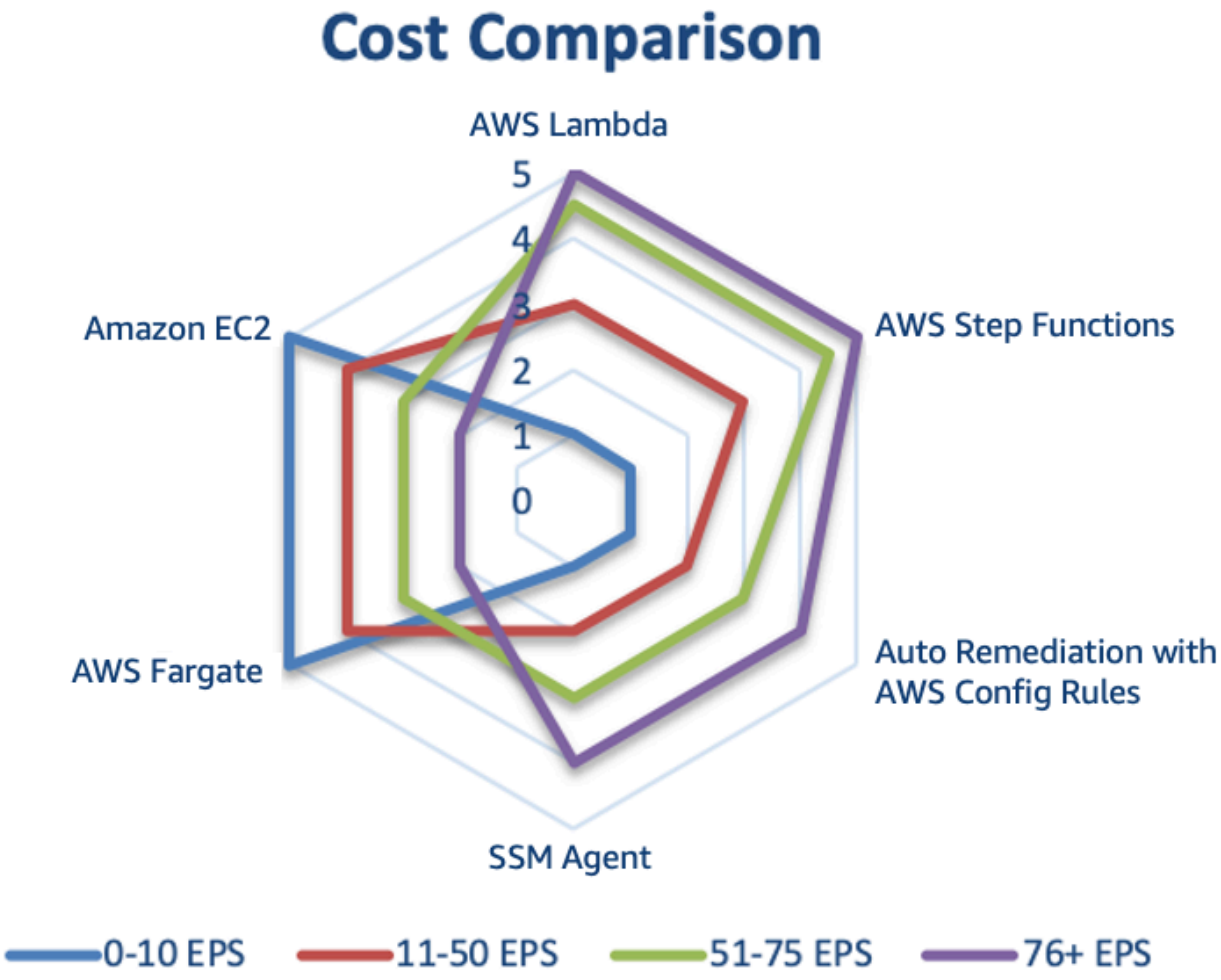


Figura 5: Confronto dei costi dei metodi di scansione delle opzioni di automazione (eventi al secondo [EPS])

## Risposta basata sugli eventi

Tramite un sistema di risposta basata sugli eventi, un meccanismo di rilevazione attiva un meccanismo di risposta per correggere automaticamente l'evento. Puoi utilizzare le funzionalità di

risposta basata sugli eventi per ridurre il time-to-value tra meccanismi di rilevazione e di risposta. Per creare questa architettura basata sugli eventi, puoi utilizzare AWS Lambda, un servizio di calcolo serverless che esegue il codice in risposta a eventi e gestisce automaticamente le risorse di calcolo sottostanti per tuo conto.

Ad esempio, supponiamo che tu disponga di un account AWS con il servizio AWS CloudTrail abilitato. Se AWS CloudTrail viene disabilitato (tramite l'API `cloudtrail:StopLogging`), la procedura di risposta consiste nell'abilitare nuovamente il servizio e indagare sull'utente che ha disabilitato la registrazione di AWS CloudTrail. Invece di eseguire questi passaggi manualmente in AWS Management Console, è possibile abilitare nuovamente la registrazione a livello di codice (tramite l'API `cloudtrail:StartLogging`). Se lo implementi con il codice, il tuo obiettivo di risposta è eseguire questa attività il più rapidamente possibile e notificare ai team di risposta che la risposta è stata eseguita.

Per eseguire queste attività, è possibile scomporre la logica in un semplice codice da eseguire in una funzione AWS Lambda. È quindi possibile utilizzare Amazon CloudWatch Events per monitorare l'evento `cloudtrail:StopLogging` specifico e richiamare la funzione se l'evento si verifica. Quando questa funzione del risponditore AWS Lambda viene richiamata da Amazon CloudWatch Events, è possibile trasmetterle i dettagli dell'evento specifico con le informazioni del principale che ha disabilitato AWS CloudTrail, quando è stato disabilitato, della risorsa specifica interessata e altre informazioni pertinenti. È possibile utilizzare queste informazioni per ampliare il risultato dei registri e quindi generare una notifica o un avviso con solo i valori specifici richiesti da un analista della risposta.

Idealmente, l'obiettivo della risposta guidata dagli eventi è che la funzione del risponditore Lambda esegua le attività di risposta e quindi notifichi al risponditore che l'anomalia è stata risolta con successo con qualsiasi informazione contestuale pertinente. Spetta quindi all'addetto alle risposte decidere come determinare perché si è verificato e come prevenire le ricorrenze future. Questo circuito di feedback favorisce un ulteriore miglioramento della sicurezza negli ambienti cloud. Per raggiungere questo obiettivo, è necessario disporre di una cultura che consenta al team di sicurezza di lavorare più a stretto contatto con i team di sviluppo e operativi.

# Esempi di risposte agli incidenti

Argomenti



## Incidenti nell'ambito del servizio

Gli incidenti nell'ambito del servizio sono generalmente gestiti esclusivamente tramite le API di AWS.

### Identità

AWS fornisce API ai nostri servizi cloud che vengono utilizzate da milioni di clienti per costruire nuove applicazioni e ottenere risultati aziendali. Queste API possono essere richiamate attraverso molti metodi, ad esempio dai software development kit (SDK), da AWS CLI e dalla AWS Management Console. Per interagire con AWS attraverso questi metodi, il servizio IAM aiuta a controllare in modo sicuro l'accesso alle risorse AWS. Utilizza IAM per controllare chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) per l'utilizzo di risorse a livello di account. Per un elenco dei servizi AWS che puoi utilizzare con IAM, consulta Servizi AWS che funzionano con IAM.

Quando crei un account AWS per la prima volta, inizi con una singola identità single sign-on (SSO) che ha accesso completo a tutti i servizi e le risorse AWS nell'account. Tale identità è detta utente root dell'account AWS e puoi accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane, e in particolare non per le attività amministrative. Ti consigliamo invece di seguire la best practice di utilizzare l'utente root solo per creare il primo utente IAM, archiviare in modo sicuro le credenziali dell'utente root ed eseguire solo alcune attività di gestione degli account e dei servizi. Per ulteriori informazioni, consulta la sezione relativa alla creazione di utenti IAM singoli.

Sebbene queste API forniscano valore a milioni di clienti, alcune di esse possono essere utilizzate in modo illecito se persone sbagliate ottengono l'accesso al tuo account IAM o alle credenziali root. Ad esempio, puoi utilizzare le API per abilitare la registrazione all'interno dell'account, ad esempio AWS CloudTrail. Tuttavia, se gli aggressori ottengono le tue credenziali, possono anche utilizzare l'API per disabilitare questi registri. È possibile prevenire questo tipo di uso illecito configurando le autorizzazioni IAM appropriate che seguono un modello con privilegi minimi e proteggendo adeguatamente le credenziali IAM. Per ulteriori informazioni, consulta IAM Best Practices (Best

practice IAM) nella Guida per l'utente di AWS Identity and Access Management. Se si verifica questo tipo di evento, sono disponibili diversi controlli di rilevazione per stabilire che la registrazione AWS CloudTrail è stata disabilitata, tra cui AWS CloudTrail, AWS Config, AWS Trusted Advisor, Amazon GuardDuty e AWS CloudWatch Events.

### Risorse

Altre caratteristiche che possono essere utilizzate in modo illecito o configurate in modo errato variano da organizzazione a organizzazione, in base al modo in cui ogni cliente opera nel cloud. Ad esempio, alcune organizzazioni intendono rendere accessibili al pubblico determinati dati o applicazioni, mentre altre mantengono le loro applicazioni e dati interni e riservati. Non tutti gli eventi di sicurezza sono di natura dannosa; alcuni eventi potrebbero derivare da configurazioni involontarie o improprie. Valuta quali API o caratteristiche un forte impatto sulla tua organizzazione e se le usi frequentemente o raramente.

Utilizzando strumenti e servizi, è possibile identificare molte configurazioni di sicurezza errate. Ad esempio, AWS Trusted Advisor fornisce una serie di controlli per le best practice. I partner APN offrono inoltre centinaia di prodotti leader nel settore che sono equivalenti, identici o si integrano ai controlli esistenti negli ambienti On-Premise. Alcuni di questi prodotti e soluzioni sono stati prequalificati dal programma AWS Partner Competency. Ti invitiamo a visitare la sezione relativa all'analisi della configurazione e delle vulnerabilità del programma APN Security Competency per esplorare queste soluzioni e determinare se sono in grado di soddisfare i tuoi requisiti.

## Incidenti nell'ambito dell'infrastruttura

L'ambito dell'infrastruttura include in genere i dati dell'applicazione o l'attività correlata alla rete, ad esempio il traffico verso le istanze Amazon EC2 all'interno VPC e i processi in esecuzione nei sistemi operativi delle istanze Amazon EC2.

Ad esempio, supponiamo che la soluzione di monitoraggio abbia notificato una potenziale anomalia di sicurezza nella tua istanza Amazon EC2. Le seguenti operazioni sono passaggi comuni per risolvere questo problema:

1. Acquisisci i metadati dall'istanza Amazon EC2 prima di apportare modifiche al tuo ambiente.
2. Proteggi l'istanza Amazon EC2 dall'interruzione accidentale abilitando la protezione dall'interruzione dell'istanza.
3. Isola l'istanza Amazon EC2 cambiando il gruppo di sicurezza VPC. Tuttavia, tieni presente il tracciamento della connessione VPC e altre tecniche di contenimento.

4. Distacca l'istanza Amazon EC2 da qualsiasi gruppo AWS Auto Scaling.
5. Annulla la registrazione dell'istanza Amazon EC2 da qualsiasi servizio di bilanciamento del carico elastico correlato.
6. Crea un snapshot dei volumi di dati di Amazon EBS collegati all'istanza EC2 per la conservazione e le indagini di follow-up.
7. Aggiungi un tag all'istanza Amazon EC2 come messa in quarantena per l'indagine e aggiungi eventuali metadati pertinenti, come il trouble ticket associato all'indagine.

Puoi eseguire tutti i passaggi precedenti utilizzando le API AWS, gli SDK AWS, l'AWS CLI e la AWS Management Console. Per interagire con AWS utilizzando questi metodi, il servizio IAM aiuta a controllare in modo sicuro l'accesso alle risorse AWS. L'utente utilizza IAM per controllare chi è autenticato e autorizzato a utilizzare le risorse a livello di account. Il servizio IAM fornisce l'autenticazione e l'autorizzazione per eseguire queste operazioni e interagire con l'ambito del servizio.

Uno snapshot di un volume Amazon EBS è una copia point-in-time a livello di blocco di un volume di dati EBS, che si verifica in modo asincrono e potrebbe richiedere del tempo per essere completata, ma rappresenta un delta di tali dati in futuro. È possibile creare nuovi volumi EBS da queste copie e montarli sull'istanza EC2 forense per un'analisi approfondita non in linea da parte degli investigatori forensi. Il diagramma seguente mostra una versione semplificata del risultato e non descrive tutti i componenti di rete (ad esempio sottoreti, tabelle di routing e liste di controllo accessi).

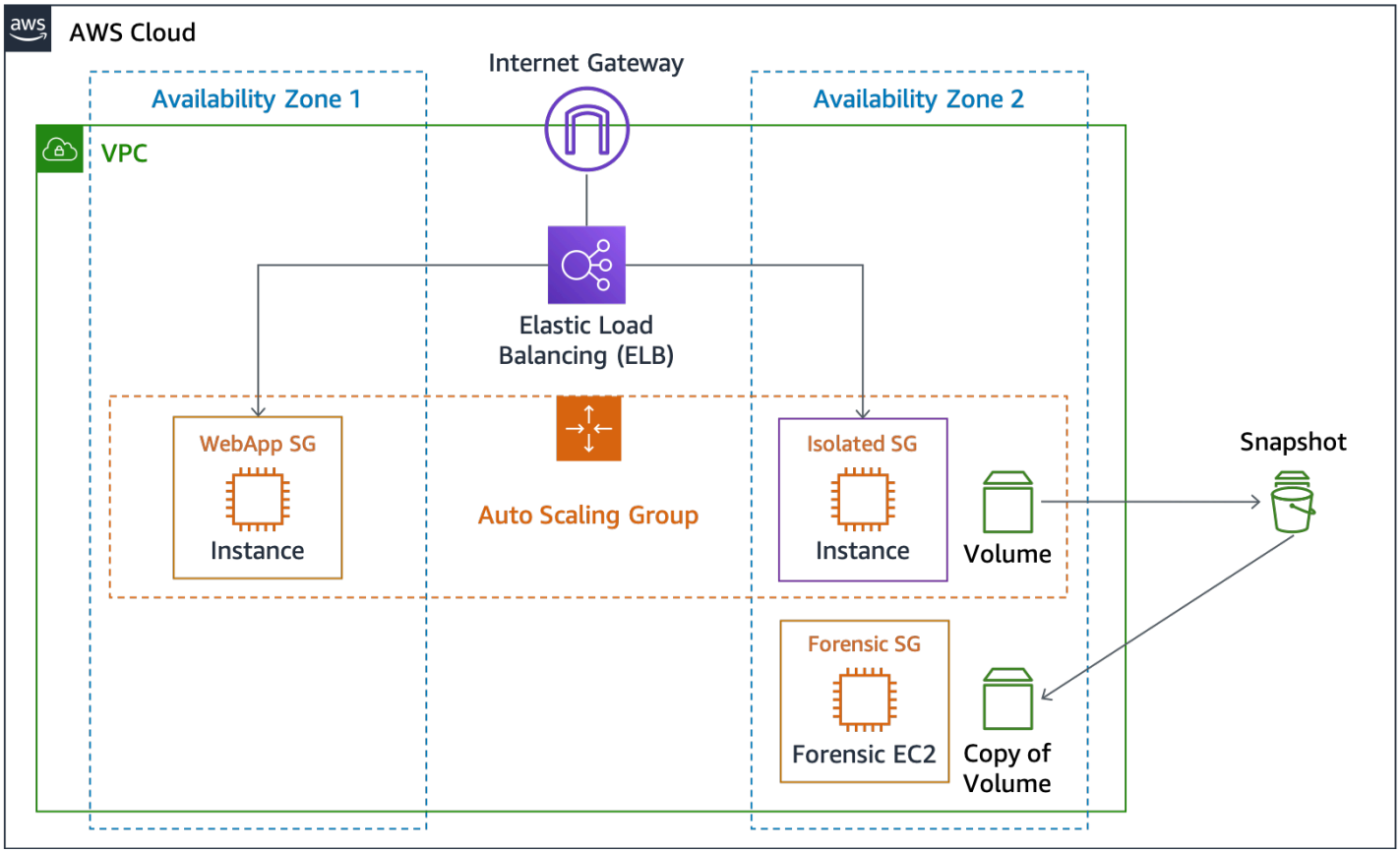


Figura 6: Isolamento e snapshot delle istanze EC2

Argomenti



## Decisioni investigative

A questo punto, puoi scegliere tra un'indagine non in linea (chiudendo immediatamente l'istanza) o un'indagine online (mantenendo l'istanza in esecuzione). Un vantaggio dell'indagine non in linea è che, dopo la chiusura dell'istanza, non può più influire sull'ambiente esistente. Inoltre, puoi creare una copia dell'istanza interessata dagli snapshot EBS ed esaminarla in un account AWS isolato con un ambiente isolato progettato specificamente per le indagini. Tuttavia, è possibile scegliere di non chiudere immediatamente l'istanza, se un'indagine online consente di acquisire prove potenzialmente volatili dal sistema operativo host, come la memoria o il traffico di rete.

## Acquisizione di dati volatili

Anche se potresti non scegliere di eseguire l'indagine online, è importante comprendere i meccanismi necessari per acquisire dati volatili da un'istanza. Un'indagine online richiede l'interazione con il sistema operativo in esecuzione sull'istanza Amazon EC2. In questo scenario, è necessario più del servizio AWS IAM per eseguire attività su un'istanza Amazon EC2. Sebbene sia possibile autenticarsi direttamente sul computer utilizzando un metodo standard (come Linux secure shell (SSH) o desktop remoto di Microsoft Windows (RDP)), l'interazione manuale con il sistema operativo non è una best practice. Si consiglia di utilizzare uno strumento di automazione a livello di programmazione per eseguire attività su un host.

## Utilizzo di AWS Systems Manager

Il Run Command di AWS Systems Manager consente di eseguire in remoto e in modo sicuro modifiche on demand eseguendo script di shell Linux e comandi di Windows PowerShell su un'istanza di destinazione. Sebbene sia possibile richiamare Run Command tramite le autorizzazioni nel servizio AWS IAM, è necessario prima attivare le istanze Amazon EC2 come istanze gestite, installare SSM Agent sui computer (se non è installato di default) e configurare le autorizzazioni AWS IAM. Se sei interessato a utilizzare Run Command per attività di automazione o risposta, assicurati di completare le attività prerequisite prima di eseguire un'indagine.

AWS Systems Manager, che include Run Command, è integrato con AWS CloudTrail, un servizio che acquisisce le chiamate API effettuate da o per conto di un Systems Manager e consegna i file di log a un bucket Simple Storage Service (Amazon S3) specificato. Le informazioni raccolte da AWS CloudTrail consentono di determinare la richiesta effettuata, l'indirizzo IP di origine che ha effettuato la richiesta, l'autore della richiesta, il momento in cui è stata effettuata e così via. CloudTrail crea registri di tutte le operazioni API di Systems Manager, incluse le richieste API di esecuzione di comandi utilizzando Run Command o per creare documenti di Systems Manager.

È possibile utilizzare il servizio Run Command di AWS Systems Manager per richiamare l'SSM Agent che esegue gli script della shell Linux e i comandi di Windows PowerShell. Questi script possono caricare ed eseguire strumenti specifici per acquisire dati aggiuntivi dall'host, come il modulo del kernel Linux Memory Extractor (LiME). È quindi possibile trasferire l'acquisizione della memoria nell'istanza forense di Amazon EC2 nella rete VPC o in un bucket Simple Storage Service (Amazon S3) per un'archiviazione durevole.

# Automatizzazione dell'acquisizione

Un metodo per richiamare l'SSM Agent consiste nel scegliere come destinazione Run Command tramite Amazon CloudWatch Events quando l'istanza è taggata con un tag specifico. Ad esempio, se si applica il tag `Response=Isolate+MemoryCapture` a un'istanza interessata, è possibile configurare Amazon CloudWatch Events per attivare due operazioni:

- Una funzione Lambda che esegua le attività di isolamento
- Un Run Command che esegua un comando shell per esportare la memoria Linux tramite l'SSM Agent.

Questa risposta basata su tag è un altro metodo di risposta guidata dagli eventi.

# Conclusione

Mentre continui il tuo percorso verso il cloud, è importante considerare i concetti di risposta fondamentali agli incidenti di sicurezza indicati in precedenza per l'ambiente AWS. Puoi combinare i controlli disponibili, le funzionalità cloud e le opzioni di correzione per aiutare a migliorare la sicurezza del tuo ambiente cloud. È inoltre possibile iniziare in piccolo e iterare man mano che si adottano funzionalità di automazione che migliorano la velocità di risposta, in modo da essere meglio preparati quando si verificano eventi di sicurezza.

# Risorse aggiuntive

Per ulteriori informazioni, consulta:

- AWS Well-Architected
- Pagina AWS Cloud Adoption Framework
- Soluzione di registrazione centralizzata AWS
- Visualizza i registri AWS CloudTrail utilizzando AWS Glue e Amazon QuickSight
- Come monitorare avvisi di un sistema di rilevamento delle intrusioni basato su host in istanze Amazon EC2
- Archiviare e monitorare file di log di OS e delle applicazioni con Amazon CloudWatch
- Identity and Access Management in Simple Storage Service (Amazon S3)
- Utilizzo del controllo delle versioni (Simple Storage Service (Amazon S3))
- Utilizzo della cancellazione MFA
- Protezione dei dati mediante la crittografia lato server con chiavi gestite da AWS KMS (SSE-KMS)
- Risposta agli incidenti con la console e la CLI AWS
- Preparazione per il California Consumer Privacy Act (CCPA)

# Media

- AWS re:Invent 2014 (SEC402): Intrusion Detection in the Cloud (Rilevamento delle intrusioni nel cloud)
- AWS re:Invent 2014 (SEC404): Incident Response in the Cloud (Risposta agli incidenti nel cloud)
- AWS re:Invent 2015 (SEC308): Wrangling Security Events in The Cloud (Organizzazione di eventi di sicurezza nel cloud)
- AWS re:Invent 2015 (SEC316): Harden Your Architecture with Security Incident Response Simulations (Rafforzare l'architettura con simulazioni di risposta agli incidenti di sicurezza)
- AWS re:Invent 2016 (SEC313): Automating Security Event Response, from Idea to Code to Execution (Automatizzare la risposta agli eventi di sicurezza, dall'idea al codice fino all'esecuzione)
- AWS re:Invent 2017 (SID302): Force Multiply Your Security Team with Automation and Alexa (Forzare la moltiplicazione del team di sicurezza con l'automazione e Alexa)

- AWS re:Invent 2016 (SAC316): Security Automation: Spend Less Time Securing Your Applications (Automazione della sicurezza: dedica meno tempo alla protezione delle applicazioni)
- AWS re:Invent 2016 (SAC304): Predictive Security: Using Big Data to Fortify Your Defenses (Sicurezza predittiva: utilizzare i big data per rafforzare le difese)
- AWS re:Invent 2017 (SID325): Amazon Macie: Data Visibility Powered by Machine Learning for Security and Compliance Workloads (Amazon Macie: Visibilità dei dati basata sull'apprendimento automatico per carichi di lavoro di sicurezza e conformità)
- AWS London Summit 2018: Automating Incident Response and Forensics in AWS (Automatizzazione della risposta agli incidenti e delle analisi forensi in AWS)

## Strumenti di terze parti

I seguenti link a strumenti di terze parti sono esterni e non sono approvati da AWS. AWS non offre garanzie o dichiarazioni di alcun tipo su questi strumenti o pagine.

- AWS_IR: utility della riga di comando installabile in Python per l'attenuazione delle compromissioni tra host e chiavi.
- MargaritaShotgun: strumento di acquisizione di memoria remota.
- ThreatPrep: modulo Python per la valutazione delle best practice degli account AWS relative alla preparazione alla gestione degli incidenti.
- ThreatResponse Web: piattaforma di analisi basata sul Web da utilizzare con gli strumenti a riga di comando AWS_IR.
- GRR Rapid Response: analisi forense in tempo reale per la risposta agli incidenti.
- Linux Write Blocker: patch del kernel e gli strumenti dello spazio utente per abilitare il blocco della scrittura del software Linux.

## Riferimenti di settore

- NIST SP 800-61R2: Guida alla gestione degli incidenti di sicurezza informatica

# Revisioni del documento

Per ricevere una notifica sugli aggiornamenti di questo whitepaper, iscriviti al feed RSS.

| update-history-change | update-history-description | update-history-date |
| --- | --- | --- |
| Aggiornamenti minori | Correzioni di bug e varie modifiche minori. | 2 giugno 2021 |
| Aggiornamento di minore entità | Link interrotti corretti. | 5 marzo 2021 |
| Whitepaper aggiornato | Collegamenti interrotti corretti e numerose modifiche al testo per migliorare la leggibilità. | 23 novembre 2020 |
| Aggiornamento di minore entità | Collegamento corretto a "Incident Response with AWS Console and CLI" (Risposta agli incidenti con la console e la CLI AWS). | 30 giugno 2020 |
| Whitepaper aggiornato | Aggiornato per nuovi servizi di sicurezza, intelligence sulle minacce, responsab ilità condivisa per container , automazione e CCPA. Aggiunte le appendici con albero decisionale di esempio e runbook. | 11 giugno 2020 |
| Pubblicazione iniziale | Prima pubblicazione del whitepaper | 1 giugno 2019 |

# Appendice A: definizioni delle capacità del cloud

AWS offre oltre 150 servizi cloud e migliaia di caratteristiche. Molti di questi forniscono funzionalità di rilevazione, preventive e reattive native, mentre altri possono essere utilizzati per progettare soluzioni di sicurezza personalizzate. Questa sezione include un sottoinsieme di quei servizi più rilevanti per la risposta agli incidenti nel cloud.

Argomenti



## Registrazione ed eventi

AWS CloudTrail: AWS CloudTrail è un servizio che abilita la governance, la conformità, la verifica operativa e dei rischi del tuo account AWS. Con CloudTrail puoi registrare, monitorare in modo continuo e mantenere le attività dell'account correlate alle operazioni all'interno dell'infrastruttura AWS. CloudTrail fornisce una cronologia degli eventi delle attività dell'account AWS, incluse le operazioni eseguite tramite la AWS Management Console, gli SDK AWS, strumenti a riga di comando e altri servizi AWS. La cronologia degli eventi semplifica l'analisi di sicurezza, il monitoraggio delle modifiche delle risorse e la risoluzione dei problemi.

I file di log convalidati sono preziosi nelle indagini forensi e per la sicurezza. Per determinare se un file di log è stato modificato, eliminato o modificato dopo che CloudTrail lo ha distribuito, utilizzare la convalida dell'integrità dei file di log di CloudTrail. Questa caratteristica è integrata mediante algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende impossibile, a livello di programmazione, qualsiasi operazione di modifica, eliminazione o contraffazione dei file di log di CloudTrail senza che tale operazione venga rilevata.

Di default, i file di log inviati da CloudTrail al tuo bucket vengono crittografati mediante la crittografia lato server di Amazon. Facoltativamente è possibile utilizzare le chiavi gestite AWS Key Management Service (AWS KMS) (SSE-KMS) per i file di log di CloudTrail.

Amazon CloudWatch Events: Amazon CloudWatch Events fornisce un flusso quasi in tempo reale di eventi di sistema che descrivono le modifiche nelle risorse AWS o quando le chiamate API vengono pubblicate da AWS CloudTrail. Utilizzando semplici regole che puoi impostare rapidamente, puoi abbinare eventi e instradarli verso una o più funzioni o flussi target. CloudWatch Events rileva le modifiche operative appena si verificano. CloudWatch Events risponde a queste modifiche operative e prende le necessarie misure correttive inviando messaggi per rispondere all'ambiente, attivando funzioni, apportando modifiche, e acquisendo informazioni sullo stato. Alcuni servizi di sicurezza, come Amazon GuardDuty, producono il loro output sotto forma di CloudWatch Events.

AWS Config: AWS Config è un servizio che consente di valutare e verificare le configurazioni delle risorse AWS. Config monitora e registra continuamente le configurazioni delle risorse AWS e permette di automatizzare la valutazione delle configurazioni registrate e le impostazioni desiderate. Con Config, puoi esaminare le modifiche nelle configurazioni e le relazioni tra le risorse AWS, manualmente o automaticamente. È possibile esaminare le cronologie dettagliate della configurazione delle risorse e determinare la conformità generale rispetto alle configurazioni specificate nelle linee guida interne. Ciò permette di semplificare le operazioni di verifica della conformità, l'analisi della sicurezza, la gestione delle modifiche e risoluzione dei problemi operativi.

Registri di accesso di Simple Storage Service (Amazon S3): se archivi informazioni sensibili in un bucket Simple Storage Service (Amazon S3), puoi abilitare i registri di accesso S3 per registrare ogni caricamento, download e modifica di tali dati. Questo registro è separato e in aggiunta ai log di CloudTrail che registrano le modifiche al bucket stesso (come la modifica delle policy di accesso e delle policy del ciclo di vita).

Amazon CloudWatch Logs: puoi utilizzare Amazon CloudWatch Logs per monitorare, archiviare e accedere ai file di log (come il sistema operativo, l'applicazione e i file di log personalizzati) dalle istanze Amazon Elastic Compute Cloud (Amazon EC2) utilizzando l'agente CloudWatch Logs. Inoltre, Amazon CloudWatch Logs può acquisire log da AWS CloudTrail, query DNS di Amazon Route 53, flusso di log del VPC, funzioni Lambda e altre fonti. I dati dei registri associati possono quindi essere recuperati da CloudWatch Logs.

Flussi di log di Amazon VPC: i flussi di log del VPC consentono di acquisire le informazioni sul traffico IP da e per le interfacce di rete nel VPC. Dopo aver creato un flusso di log, è possibile visualizzare e recuperare i relativi dati in Amazon CloudWatch Logs. I flussi di log del VPC possono essere utili per diverse attività. Ad esempio, puoi utilizzare i flussi di log per risolvere il motivo per cui il traffico specifico non raggiunge un'istanza, il che può aiutare a diagnosticare regole del gruppo di sicurezza eccessivamente restrittive. Puoi anche utilizzare i flussi di log come uno strumento di sicurezza per monitorare il traffico che raggiunge l'istanza.

Registri AWS WAF: AWS WAF ora supporta la registrazione completa di tutte le richieste Web ispezionate dal servizio. È possibile archiviare tali registri in Simple Storage Service (Amazon S3) per necessità di conformità e di verifica, nonché utilizzarli per il debug e per ulteriori analisi forensi. I registri consentiranno di comprendere quali sono le regole attivate e perché alcune richieste Web vengono bloccate. È anche possibile integrare i log con gli strumenti SIEM e di analisi dei registri.

Altri registri AWS: con il ritmo dell'innovazione, continuiamo a implementare nuove caratteristiche e funzionalità per i clienti praticamente ogni giorno, il che significa che sono disponibili dozzine di servizi AWS che forniscono funzionalità di registrazione e monitoraggio. Per informazioni sulle caratteristiche disponibili per ciascun servizio AWS, consulta la documentazione AWS relativa al servizio.

## Visibilità e avvisi

AWS Security Hub: AWS Security Hub offre una vista completa degli avvisi di sicurezza ad alta priorità e dello stato di conformità tra gli account AWS. Grazie a Security Hub hai a disposizione una posizione unica che aggrega, organizza e assegna le priorità agli avvisi di sicurezza, o ai risultati, provenienti da diversi servizi AWS come Amazon GuardDuty, Amazon Inspector e Amazon Macie, oltre che dalle soluzioni dei partner AWS. I risultati sono raccolti visivamente nei pannelli di controllo integrati con grafici e tabelle concreti. Inoltre, puoi monitorare in modo costante il tuo ambiente tramite i controlli di conformità automatizzati che si basano sulle best practice di AWS e sugli standard di settore in linea con la tua organizzazione.

Amazon GuardDuty: Amazon GuardDuty è un servizio gestito di rilevazione delle minacce che monitora costantemente possibili comportamenti dannosi o non autorizzati così da proteggere i tuoi account e i tuoi carichi di lavoro su AWS. Monitora attività sospette quali chiamate API inusuali o implementazioni potenzialmente non autorizzate, le quali indicano che l’account potrebbe esser stato compromesso. GuardDuty, inoltre, rileva le istanze potenzialmente compromesse o un attacco di ricognizione (reconnaissance).

GuardDuty individua malintenzionati sospetti attraverso feed integrati di intelligence sulle minacce e utilizza il machine learning per rilevare anomalie nelle attività di account e carichi di lavoro. Quando viene rilevata una potenziale minaccia, il servizio inoltra un avviso di sicurezza dettagliato alla console di GuardDuty e ad AWS CloudWatch Events. In questo modo è possibile tradurre gli avvisi in azioni concrete, integrandoli in sistemi di gestione di eventi e flussi di lavoro esistenti.

Amazon Macie: Amazon Macie è un servizio di sicurezza basato sull'IA che aiuta a prevenire la perdita di dati perché rileva, classifica e protegge i dati sensibili archiviati in AWS. Amazon

Macie utilizza il machine learning per riconoscere dati sensibili quali le informazioni personali di identificazione (PII) o la proprietà intellettuale, vi assegna un valore aziendale e fornisce visibilità su relativi percorsi di archiviazione e modalità di utilizzo dei dati nell'organizzazione. Amazon Macie monitora in modo continuo le attività di accesso ai dati per rilevare eventuali anomalie, inviando avvisi quando individua un rischio di accesso non autorizzato o di divulgazione accidentale di dati.

Regole di AWS Config: una regola AWS Config rappresenta le configurazioni desiderate per una risorsa e viene valutata mettendola a confronto con le modifiche apportate alla configurazione delle risorse pertinenti, in base a quanto registrato da AWS Config. È possibile visualizzare i risultati della valutazione della regola rispetto alla configurazione di una risorsa su un pannello di controllo. Utilizzando le regole di configurazione, è possibile prendere in esame conformità e livello di rischio dal punto di vista della configurazione, consultare tendenze di conformità nel corso del tempo e individuare quale modifica alla configurazione ha causato la mancata conformità di una risorsa a una determinata regola.

AWS Trusted Advisor: AWS Trusted Advisor è una risorsa online in grado di aiutare a ridurre i costi, aumentare le prestazioni e migliorare la sicurezza, ottimizzando l'ambiente AWS. Trusted Advisor fornisce linee guida in tempo reale per consentire di effettuare il provisioning delle risorse attenendosi alle best practice di AWS. Il set completo di controlli di Trusted Advisor, inclusa l'integrazione di CloudWatch Events, è disponibile per i clienti dei piani di supporto Business ed Enterprise.

Amazon CloudWatch: Amazon CloudWatch è un servizio di monitoraggio per le risorse di AWS Cloud e le applicazioni in esecuzione su AWS. Puoi utilizzare Amazon CloudWatch per raccogliere e monitorare parametri e file di log, impostare allarmi e reagire automaticamente alle modifiche nelle risorse AWS. Amazon CloudWatch consente il monitoraggio di risorse AWS quali le istanze Amazon EC2, le tabelle Amazon DynamoDB e le istanze database di Amazon RDS, nonché i parametri personalizzati generati dalle applicazioni e dai servizi e i file di log generati dalle applicazioni. È possibile utilizzarlo anche per ottenere visibilità a livello di sistema su utilizzo delle risorse, prestazioni delle applicazioni e integrità operativa. Puoi utilizzare le informazioni dettagliate ottenute per reagire di conseguenza e mantenere le prestazioni delle applicazioni sempre ottimali.

AWS Inspector: Amazon Inspector è un servizio di valutazione della sicurezza automatizzato che aiuta a migliorare la sicurezza e la conformità delle applicazioni implementate in AWS. Amazon Inspector valuta automaticamente le applicazioni per rilevare vulnerabilità o deviazioni dalle best practice. Dopo aver eseguito una valutazione, Amazon Inspector fornisce un elenco dettagliato con i risultati della sicurezza, ordinati secondo il livello di gravità. Tali risultati possono essere consultati direttamente oppure come parte di un report di valutazione dettagliato, disponibile tramite la console o l'API di Amazon Inspector.

Amazon Detective: Amazon Detective è un servizio di sicurezza che raccoglie automaticamente i dati di registro dalle risorse AWS e utilizza il machine learning, l'analisi statistica e teoria dei grafi per costruire un set di dati collegato che permette di condurre indagini sulla sicurezza più veloci ed efficienti. Amazon Detective può analizzare trilioni di eventi da origini dati diversificate come flussi di log del cloud privato virtuale (VPC), AWS CloudTrail e Amazon GuardDuty e creare automaticamente una panoramica interattiva e unificata di risorse, utenti e delle loro interazioni nel corso del tempo. Grazie a questa panoramica unificata è possibile visualizzare tutti i dettagli e i contesti in un unica posizione per identificare le ragioni sottostanti ai risultati, analizzare le attività cronologiche rilevanti e determinare rapidamente la causa principale.

# Automazione

AWS Lambda: AWS Lambda è un servizio di calcolo serverless che esegue il codice in risposta a determinati eventi, oltre a gestire automaticamente le risorse di calcolo in uso. È possibile utilizzare Lambda per estendere altri servizi AWS con logica personalizzata oppure creare servizi back-end personalizzati operativi a livello di dimensionamento, prestazioni e sicurezza di AWS. Lambda esegue il codice su un'infrastruttura di calcolo ad elevata disponibilità ed esegue tutte le attività di amministrazione delle risorse di calcolo per conto dell'utente. Tra queste, la manutenzione del server e del sistema operativo, l'effettuazione del provisioning della capacità e la scalabilità automatica, l'implementazione di codici e patch di sicurezza e il monitoraggio e la registrazione di codici. Tutto quello che devi fare è fornire il codice.

AWS Step Functions: AWS Step Functions semplifica il coordinamento di componenti di applicazioni e microservizi distribuiti tramite flussi di lavoro visivi. Step Functions dispone di una console grafica in cui è possibile disporre e visualizzare i componenti dell'applicazione in una serie di fasi. Questo semplifica la creazione e l'esecuzione di applicazioni multifase. Step Functions attiva automaticamente e tiene traccia di ogni fase e, in caso di errore, riprova, in modo che l'applicazione venga eseguita nell'ordine e nel modo previsto.

Step Functions registra lo stato di ogni fase, per consentire, in caso di errore, di eseguire una diagnosi e risolvere i problemi rapidamente. Puoi modificare e aggiungere fasi senza scrivere codice, in modo da poter far evolvere facilmente l'applicazione e innovare più rapidamente. AWS Step Functions fa parte di AWS Serverless Platform e semplifica l'orchestrazione di funzioni AWS Lambda per applicazioni serverless. Puoi anche utilizzare Step Functions per l'orchestrazione di microservizi utilizzando risorse di calcolo quali Amazon EC2 e Amazon ECS.

AWS Systems Manager: AWS Systems Manager offre visibilità e controllo dell'infrastruttura su AWS. Systems Manager fornisce un'interfaccia utente unificata in modo da poter visualizzare i

dati operativi da più servizi AWS e consente di automatizzare le attività operative nelle risorse AWS. Con Systems Manager, è possibile raggruppare le risorse per applicazione, visualizzare i dati operativi per il monitoraggio e la risoluzione dei problemi e agire sui gruppi di risorse. Systems Manager può mantenere le istanze nel loro stato definito, eseguire modifiche alle istanze on demand, come l'aggiornamento di applicazioni o l'esecuzione di script di shell ed eseguire altre attività di automazione e patch.

## Archiviazione sicura

Simple Storage Service (Amazon S3): Simple Storage Service (Amazon S3) è un'archiviazione di oggetti per archiviare e recuperare qualsiasi quantità di dati da qualsiasi origine. È stato progettato per offrire una durabilità del 99,999999999% e archiviare dati per milioni di applicazioni utilizzate dai leader di mercato di ogni settore. Simple Storage Service (Amazon S3) offre una sicurezza completa ed è progettato per soddisfare i requisiti normativi. Fornisce ai clienti la flessibilità nei metodi utilizzati per la gestione dei dati per ottimizzare i costi, controllare gli accessi e assicurare la conformità. Simple Storage Service (Amazon S3) offre funzionalità di query-in-place, che consente di eseguire potenti analisi dei dati direttamente sui dati a riposo in Amazon S3. Simple Storage Service (Amazon S3) è il servizio di archiviazione nel cloud maggiormente supportato, grazie all'integrazione dalla community più grande di soluzioni di terze parti e partner integratori di sistemi e agli altri servizi AWS.

Amazon S3 Glacier: Amazon S3 Glacier è un servizio di archiviazione nel cloud sicuro, duraturo ed estremamente economico per l'archiviazione dei dati e il backup a lungo termine. È progettato per offrire una durabilità del 99,999999999%, offre una sicurezza completa ed è progettato per soddisfare i requisiti normativi. Amazon S3 Glacier fornisce funzionalità di query-in-place che permette di eseguire analisi dei dati potenti direttamente sui dati a riposo archiviati. Per mantenere i costi bassi senza diminuire la qualità del servizio, Amazon S3 Glacier offre tre opzioni per accedere agli archivi, con tempi che vanno da pochi minuti a diverse ore.

## Personalizzazione

I servizi e le caratteristiche indicate un precedenza non sono un elenco esaustivo. AWS aggiunge continuamente nuove funzionalità. Per ulteriori informazioni, ti invitiamo a consultare le pagine Novità di AWS e Sicurezza di AWS Cloud. Oltre ai servizi di sicurezza offerti da AWS come servizi cloud nativi, potresti essere interessato a costruire le tue proprie funzionalità con i servizi AWS.

Sebbene consigliamo di abilitare un set base di servizi di sicurezza all'interno dei tuoi account, come AWS CloudTrail, Amazon GuardDuty e Amazon Macie, alla fine potresti voler estendere queste

funzionalità per ricavare ulteriore valore dalle tue risorse di registro. Sono disponibili numerosi strumenti per i partner, come quelli elencati nel nostro programma APN Security Competency. Potresti anche voler scrivere le tue query per effettuare ricerche nei registri. Con l'ampio numero di servizi gestiti offerti da AWS, questo non è mai stato così semplice. Esistono molti servizi AWS aggiuntivi che possono aiutare nelle indagini che non rientrano nell'ambito di questo documento, come Amazon Athena, Amazon OpenSearch Service, Amazon QuickSight, Amazon Machine Learning e Amazon EMR.

# Appendice B: codice di esempio

## Esempio di evento AWS CloudTrail

L'esempio seguente mostra che un utente IAM denominato `Alice` ha utilizzato AWS CLI per richiamare `StopInstancesaction` di Amazon EC2 utilizzando `ec2-stop-instances`.

```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21:01:59Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "ec2-api-tools 1.6.12.2",
    "requestParameters": {
        "instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]},
        "force": false
    },
    "responseElements": {"instancesSet": {"items": [{
        "instanceId": "i-ebeaf9e2",
        "currentState": {
            "code": 64,
            "name": "stopping"
        },
        "previousState": {
            "code": 16,
            "name": "running"
        }
    }]}}
}]}
```

# Esempio di evento AWS CloudWatch

Il seguente esempio di evento Amazon CloudWatch mostra che un utente AWS IAM denominato `jane-roe-test` è stato trovato pubblicamente esposto su `www.github.com` e potrebbe essere oggetto di usi illeciti da parte di utenti non autorizzati.

```
{
  "check-name": "Exposed Access Keys",
  "check-item-detail": {
    "Case ID": "02648f3b-e18f-4019-8d68-ce25efe080ff",
    "Usage (USD per Day)": "0",
    "User Name (IAM or Root)": "jane-roe-test",
    "Deadline": "1440453299248",
    "Access Key ID": "AKIAIOSFODNN7EXAMPLE",
    "Time Updated": "1440021299248",
    "Fraud Type": "Exposed",
    "Location": "www.github.com"
  },
  "status": "ERROR",
  "resource_id": "",
  "uuid": "cce6d28f-e44b-4e61-aba1-5b4af96a0f59"
}
```

# Esempio di attività CLI nell'ambito dell'infrastruttura

I seguenti comandi dell'AWS CLI mostrano un esempio di risposta a un evento all'interno dell'ambito dell'infrastruttura. Questo esempio utilizza le API AWS per eseguire molte delle attività iniziali di risposta agli incidenti descritte in questo documento.

```
# Anomaly detected on IP X.X.X.X. Capture that instance's metadata
> aws ec2 describe-instances --filters "Name=ip-address,Values=X.X.X.X"
```

```
# Protect that instance from accidental termination
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --attribute
 disableApiTermination --value true
```

```
# Switch the EC2 instance's Security Group to a restricted Security Group
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --groups sg-a1b2c3d4
```

```
# Detach from the Auto Scaling Group
> aws autoscaling detach-instances --instance-ids i-abcd1234 --auto-scaling-group-name
 web-asg
```

```
# Deregister the instance from the Elastic Load Balancer
> aws elb deregister-instances-from-load-balancer --instances i-abcd1234 --load-
balancer-name web-load-balancer
```

```
# Create an EBS snapshot
> aws ec2 create-snapshot --volume vol-12xxxx78 --description "ResponderName-Date-
REFERENCE-ID"
```

```
# Create a new EC2 instance from the Forensic Workstation AMI
> aws ec2 run-instances --image-id ami-4n6x4n6x --count 1 --instance-type c4.8xlarge --
key-name forensicPublicKey --security-group-ids sg-1a2b3c4d --subnet-id subnet-6e7f819e
```

```
# Create a new EBS volume copy from the EBS snapshot
> aws ec2 create-volume --region us-east-1 --availability-zone us-east-1a --snapshot-id
 snap-abcd1234 --volume-type io1 --iops 10000
```

```
# Attach the volume to the forensic workstation
> aws ec2 attach-volume --volume-id vol-1234abcd --instance-id i-new4n6x --device /dev/
sdf
```

```
# Create a security group rule to allow the new Forensic Workstation to communicate to
 the contaminated instance.
> aws ec2 authorize-security-group-ingress --group-id sg-a1b2c3d4 --protocol tcp --port
 0-65535 --source-group sg-1a2b3c4d
```

```
# Tag the contaminated instance with the ticket or reference ID
> aws ec2 create-tags -resources i-abcd1234 -tags
 Key=Environment,Value=Quarantine:REFERENCE-ID
```

# Appendice C: runbook di esempio

Il seguente runbook di esempio rappresenta una singola voce di un runbook più grande. Questo runbook non è ufficiale e viene fornito solo come esempio. Man mano che crei i tuoi runbook, ognuno dei tuoi scenari può evolversi in elementi più grandi che hanno inizi e indicatori di compromesso diversi, ma tutti hanno risultati o operazioni simili che devono essere intrapresi. Realizzare questo cambiamento può anche aprire altre situazioni a risposte migliori o più approfondite.

## Runbook di risposta agli incidenti: utilizzo root

### Obiettivo

L'obiettivo di questo runbook è fornire indicazioni specifiche su come gestire l'utilizzo dell'account Root AWS. Questo runbook non sostituisce una strategia approfondita di risposta agli incidenti. Questo runbook si concentra sul ciclo di vita IR:

- Stabilire il controllo.
- Determinare l'impatto.
- Ripristino secondo necessità.
- Indagare sulla causa principale.
- Migliorare.

Gli indicatori di compromesso (IOC), i passaggi iniziali (fermare le perdite) e i comandi dettagliati della CLI necessari per eseguire tali passaggi sono elencati di seguito.

### Presupposti

- CLI configurata e installata.
- Il processo di reporting è già in atto.
- Trusted Advisor è attivo.
- Security Hub è attivo.

### Indicatori di compromesso

- Attività anomala per l'account.

  - Creazione di utenti IAM.
  - CloudTrail è disattivato.
  - Cloudwatch è disattivato.
  - SNS è in pausa.
  - Step Functions è in pausa.
- Avvio di AMI nuove o impreviste.
- Modifiche ai contatti sull'account.

## Passaggi per correggere: stabilire il controllo

La documentazione AWS per un possibile account compromesso richiama le attività specifiche elencate di seguito. La documentazione per un possibile account compromesso è disponibile nella sezione: What do I do if I notice unauthorized activity in my AWS account? (Cosa devo fare se noto attività non autorizzate nel mio account AWS?)

1. Contatta AWS Support e il TAM il prima possibile.
2. Cambia e ruota la password root e aggiungi un dispositivo MFA associato a root.
3. Ruota le password, le chiavi di accesso/segrete e i comandi CLI rilevanti per le fasi di correzione.
4. Esamina le operazioni intraprese dall'utente root.
5. Apri i runbook relativi a queste operazioni.
6. Chiudi l'incidente.
7. Esamina l'incidente e comprendi cosa è successo.
8. Risolvi i problemi sottostanti, implementa miglioramenti e aggiorna il runbook secondo necessità.

## Ulteriori operazioni: determinare l'impatto

Esamina gli elementi creati e le chiamate mutevoli. Potrebbero esserci elementi che sono stati creati per consentire l'accesso in futuro. Alcuni elementi da esaminare:

- Ruoli IAM per più account.
- Utenti IAM.
- Bucket S3.
- Istanze EC2.

- [L'applicazione e l'infrastruttura guideranno questo elenco.]

# Avvisi

I clienti sono responsabili della propria valutazione autonoma delle informazioni contenute in questo documento. Questo documento: (a) è solo a scopo informativo, (b) mostra le offerte e le pratiche attuali dei prodotti AWS soggette a modifiche senza preavviso, e (c) non crea alcun impegno o garanzia da parte di AWS e dei suoi affiliati, fornitori o licenziatari. I prodotti o servizi AWS sono forniti "così come sono" senza garanzie, dichiarazioni o condizioni di alcun tipo, sia esplicite che implicite. Le responsabilità e gli obblighi di AWS verso i propri clienti sono disciplinati dagli accordi AWS e il presente documento non fa parte né modifica alcun accordo tra AWS e i suoi clienti.