Guida all'implementazione

Risposta di sicurezza automatizzata su AWS

Risposta di sicurezza automatizzata su AWS: Guida all'implementazione

Table of Contents

Affronta automaticamente le minacce alla sicurezza con azioni di risposta e correzione predefinite in AWS Security Hub

Questa guida all'implementazione fornisce una panoramica della soluzione Automated Security Response on AWS, della sua architettura e dei componenti di riferimento, considerazioni per la pianificazione della distribuzione, delle fasi di configurazione per l'implementazione della soluzione Automated Security Response on AWS nel cloud Amazon Web Services (AWS).

Usa questa tabella di navigazione per trovare rapidamente le risposte a queste domande:

Se vuoi...	Leggi...
Conosci i costi di gestione di questa soluzione	Costo
Comprendi le considerazioni sulla sicurezza di questa soluzione	Sicurezza
Scopri come pianificare le quote per questa soluzione	Quote
Scopri quali regioni AWS sono supportate per questa soluzione	Regioni AWS supportate
Visualizza o scarica il CloudFormation modello AWS incluso in questa soluzione per distribuire automaticamente le risorse di infrastruttura (lo «stack») per questa soluzione	Modelli AWS CloudFormation
Accedi al codice sorgente e, facoltativamente, utilizza l'AWS Cloud Development Kit (AWS CDK) per distribuire la soluzione.	GitHub repository

La continua evoluzione della sicurezza richiede misure proattive per proteggere i dati, il che può rendere difficile, costoso e dispendioso in termini di tempo la reazione dei team addetti alla sicurezza. La soluzione Automated Security Response on AWS ti aiuta a reagire rapidamente per risolvere

i problemi di sicurezza fornendo risposte predefinite e azioni correttive basate sugli standard di conformità del settore e sulle migliori pratiche.

Automated Security Response on AWS è una soluzione AWS che funziona con AWS Security Hub per migliorare la sicurezza e aiuta ad allineare i carichi di lavoro alle best practice del pilastro della Well-Architected sicurezza (SEC10). https://docs.aws.amazon.com/wellarchitected/latest/framework/sec-10.html Questa soluzione consente ai clienti di AWS Security Hub di risolvere più facilmente i problemi di sicurezza comuni e migliorare il loro stato di sicurezza in AWS.

Puoi selezionare playbook specifici da distribuire nel tuo account principale di Security Hub. Ogni playbook contiene le azioni personalizzate, i ruoli IAM (Identity and Access Management), EventBridge le regole https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-rules.html Amazon, i documenti di automazione di AWS Systems Manager, le funzioni AWS Lambda e le funzioni AWS Step necessarie per avviare un flusso di lavoro di correzione all'interno di un singolo account AWS o su più account. Gli utenti autorizzati possono avviare le correzioni dal menu Azioni nella console AWS Security Hub Cloud Security Posture Management (CSPM), dall'interfaccia utente Web della soluzione o in modo programmatico tramite l'API della soluzione e possono correggere un risultato in tutti i loro Hub-managed account AWS Security con una sola azione. Ad esempio, puoi applicare i consigli del Center for Internet Security (CIS) AWS Foundations Benchmark, uno standard di conformità per proteggere le risorse AWS, per garantire che le password scadano entro 90 giorni e applicare la crittografia dei registri degli eventi archiviati in AWS.

> **Note**
>
> La correzione è destinata a situazioni emergenti che richiedono un'azione immediata. Questa soluzione apporta modifiche per correggere i risultati solo se avviata dall'utente tramite la console di gestione di AWS Security Hub o quando la correzione automatica è stata abilitata utilizzando la tabella Remediation Configuration DynamoDB. Per annullare queste modifiche, è necessario riportare manualmente le risorse allo stato originale.
> Quando correggi le risorse AWS distribuite come parte dello CloudFormation stack, tieni presente che ciò potrebbe causare una deriva. Quando possibile, correggi le risorse dello stack modificando il codice che definisce le risorse dello stack e aggiornando lo stack. Per ulteriori informazioni, consulta What is drift? nella Guida per l' CloudFormation utente di AWS.

Automated Security Response on AWS include le soluzioni correttive per gli standard di sicurezza definiti come parte di quanto segue:

- Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0
- CIS AWS Foundations Benchmark v1.4.0
- CIS AWS Foundations Benchmark v3.0.0
- Best practice per la sicurezza fondamentale di AWS (FSBP) v1.0.0
- Standard di sicurezza dei dati del settore delle carte di pagamento () v3.2.1 PCI-DSS
- Istituto nazionale di standard e tecnologia (NIST) SP 800-53 Rev. 5

La soluzione include anche un playbook Security Controls (SC) per la funzionalità consolidata dei risultati dei controlli di AWS Security Hub. Per ulteriori informazioni, consulta Playbooks. ??? Consigliamo di utilizzare il playbook SC insieme ai risultati di controllo consolidati in Security Hub.

Questa guida all'implementazione illustra le considerazioni sull'architettura e le fasi di configurazione per l'implementazione della soluzione Automated Security Response on AWS nel cloud AWS. Include collegamenti ai CloudFormation modelli AWS che avviano, configurano ed eseguono i servizi di calcolo, rete, storage e altri servizi AWS necessari per distribuire questa soluzione su AWS, utilizzando le migliori pratiche AWS per la sicurezza e la disponibilità.

La guida è destinata agli architetti, agli amministratori e DevOps ai professionisti dell'infrastruttura IT con esperienza pratica di architettura nel cloud AWS.

Funzionalità e vantaggi

L'Automated Security Response on AWS offre le seguenti funzionalità:

Correggi automaticamente i risultati per controlli specifici

Configura la soluzione per correggere automaticamente i risultati per controlli specifici modificando la tabella DynamoDB di configurazione della riparazione distribuita nell'account amministratore.

Correggi i risultati di più servizi di sicurezza AWS

Oltre ai risultati del controllo CSPM di AWS Security Hub, la soluzione può correggere i risultati di Amazon Inspector, Amazon e Amazon GuardDuty Macie. Il preprocessore associa ogni risultato alla correzione appropriata ed elabora sia l'AWS Security Finding Format (ASFF) che l'Open Cybersecurity Schema Framework (OCSF).

Gestisci le correzioni su più account e regioni da un'unica posizione

Da un account amministratore di AWS Security Hub configurato come destinazione di aggregazione per gli account e le regioni dell'organizzazione, avvia una correzione per un problema in qualsiasi account e regione in cui viene distribuita la soluzione.

Ricevi notifiche sulle azioni correttive e sui risultati

La soluzione viene pubblicata su un argomento di Amazon SNS quando le correzioni vengono avviate e quando hanno esito positivo o negativo. Puoi anche creare configurazioni di notifica dall'interfaccia utente Web per inviare i risultati e le correzioni via e-mail, Slack, JIRA o. ServiceNow Per ulteriori informazioni, consulta la sezione Configurazione delle notifiche. ???

Utilizza l'interfaccia utente Web per avviare, visualizzare e gestire le correzioni

È possibile abilitare l'interfaccia utente Web della soluzione durante la distribuzione dello stack di amministrazione. L'interfaccia utente Web offre una visualizzazione completa e intuitiva per eseguire le correzioni e visualizzare tutte le correzioni precedenti eseguite dalla soluzione.

Effettua l'integrazione con sistemi di ticket come Jira o ServiceNow

Per aiutare la tua organizzazione a reagire alle correzioni (ad esempio, l'aggiornamento del codice dell'infrastruttura), questa soluzione può inviare i ticket al tuo sistema di ticketing esterno.

Utilizza le AWSConfigRemediations partizioni in the GovCloud e China

Alcune delle correzioni incluse nella soluzione sono riconfezionamenti di AWS-owned AWSConfigRemediation documenti disponibili nella partizione commerciale ma non in Cina. GovCloud Implementa questa soluzione per utilizzare questi documenti in quelle partizioni.

Estendi la soluzione con soluzioni di correzione personalizzate e implementazioni Playbook

La soluzione è progettata per essere estensibile e personalizzabile. Per specificare un'implementazione alternativa di riparazione, distribuisci documenti di automazione AWS Systems Manager personalizzati e ruoli AWS IAM. Per supportare un set di controlli completamente nuovo che non è implementato dalla soluzione, distribuisci un Playbook personalizzato.

Per accelerare la creazione di queste personalizzazioni, la soluzione fornisce l'AI Toolkit for Custom Remediations. Il toolkit fornisce le best practice ASR, i guardrail e i modelli di sviluppo sotto forma di prompt di istruzioni da fornire a un assistente AI nel tuo ambiente di sviluppo integrato (IDE), fornendo all'assistente il contesto di cui ha bisogno per aiutarti a creare correzioni personalizzate pronte per la produzione in modo più efficiente e sicuro.

Casi d’uso

Applica la conformità a uno standard in tutti gli account e le regioni della tua organizzazione

Implementa il Playbook per uno standard (ad esempio, AWS Foundational Security Best Practices) per poter utilizzare le correzioni fornite. Avvia automaticamente o manualmente le correzioni per le risorse in qualsiasi account e regione in cui viene distribuita la soluzione per correggere le risorse che non sono conformi.

Implementa soluzioni correttive o playbook personalizzati per soddisfare le esigenze di conformità della tua organizzazione

Usa i componenti Orchestrator forniti come framework. Crea soluzioni correttive personalizzate per affrontare le risorse non conformi in base alle esigenze specifiche della tua organizzazione.

Concetti e definizioni

Questa sezione descrive i concetti chiave e definisce la terminologia specifica di questa soluzione:

riparazione, manuale di riparazione

Un'implementazione di una serie di passaggi che risolve un problema. Ad esempio, una correzione per il controllo Security Control (SC) Lambda.1 «Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico» modificherebbe la politica della funzione AWS Lambda pertinente per rimuovere le dichiarazioni che consentono l'accesso pubblico.

runbook di controllo

Uno di una serie di documenti di automazione di AWS Systems Manager (SSM) utilizzati da Orchestrator per indirizzare una correzione avviata per un controllo specifico al runbook di riparazione corretto. Ad esempio, le correzioni per SC Lambda.1 e AWS Foundational Security Best Practices (FSBP) vengono implementate con lo stesso runbook di correzione. Lambda.1 L'Orchestrator richiama il runbook di controllo per ogni controllo, denominati rispettivamente _ e _2.0.0_. ASR-AFSBP Lambda.1 ASR-SC Lambda.1 Ogni runbook di controllo richiama lo stesso runbook di riparazione, che in questo caso lo sarebbe. ASR-RemoveLambdaPublicAccess

orchestratore

Le Step Functions distribuite dalla soluzione che prendono come input un oggetto di ricerca da AWS Security Hub e richiamano il runbook di controllo corretto nell'account e nella regione di destinazione.

L'Orchestrator notifica inoltre alla soluzione SNS Topic quando la correzione viene avviata e quando la correzione ha esito positivo o negativo.

standard

Un gruppo di controlli definito da un'organizzazione come parte di un framework di conformità. Ad esempio, uno degli standard supportati da AWS Security Hub e da questa soluzione è AWS FSBP.

controllo

Una descrizione delle proprietà che una risorsa dovrebbe o non dovrebbe avere per essere conforme. Ad esempio, il controllo AWS FSBP Lambda.1 afferma che AWS Lambda Functions dovrebbe vietare l'accesso pubblico. Una funzione che consenta l'accesso pubblico fallirebbe questo controllo.

risultati di controllo consolidati, controllo di sicurezza, visualizzazione dei controlli di sicurezza

Una funzionalità di AWS Security Hub che, una volta attivata, mostra i risultati con i relativi ID di controllo consolidati anziché con gli ID che corrispondono a uno standard particolare. Ad esempio, i controlli AWS FSBP S3.2, CIS v1.2.0 2.3, CIS v1.4.0 2.1.5.2 e PCI-DSS v3.2.1 sono S3.1 tutti riconducibili al controllo consolidato (SC) «I buckets S3 dovrebbero vietare l'accesso pubblico in lettura». S3.2 Quando questa funzionalità è attivata, vengono utilizzati i runbook SC.

[Solution Web UI] amministratore delegato

Nel contesto dell'interfaccia utente Web della soluzione, un amministratore delegato è un utente che è stato invitato dall'amministratore e ha pieno accesso all'esecuzione delle correzioni e alla visualizzazione della cronologia delle correzioni. Questo utente può anche visualizzare e gestire altri utenti dell'Account Operator.

operatore dell'account [Solution Web UI]

Nel contesto dell'interfaccia utente Web della soluzione, un operatore di account è un utente invitato da un amministratore o da un amministratore delegato ad accedere all'interfaccia utente Web della soluzione. Questo utente è associato a un elenco di ID account AWS fornito nell'invito; può eseguire le correzioni e visualizzare la cronologia delle correzioni solo per quanto riguarda le risorse di questi account.

Per un riferimento generale ai termini AWS, consulta il glossario AWS.

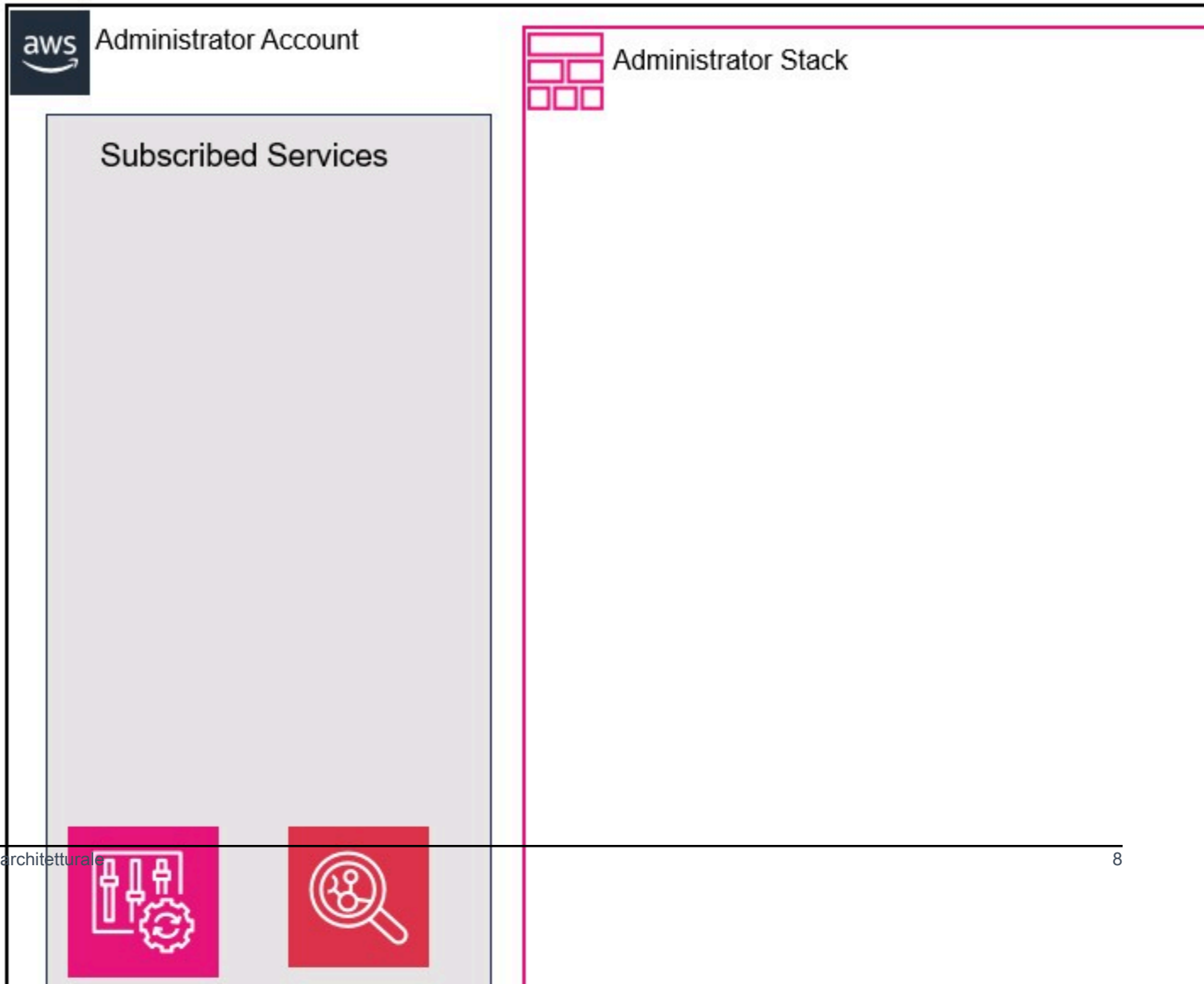
Panoramica dell’architettura

Questa sezione fornisce un diagramma dell'architettura di implementazione di riferimento per i componenti distribuiti con questa soluzione.

Diagramma architetturale

L'implementazione di questa soluzione con i parametri predefiniti crea il seguente ambiente nel cloud AWS.

Risposta di sicurezza automatizzata sull'architettura AWS


Administrator Account
Administrator Stack
Subscribed Services

> **Note**
>
> Le CloudFormation risorse AWS vengono create dai costrutti AWS Cloud Development Kit (AWS CDK).

Il flusso di alto livello per i componenti della soluzione distribuiti con il modello AWS è CloudFormation il seguente:

1. Rileva: AWS Security Hub offre ai clienti una visione completa del loro stato di sicurezza AWS. Li aiuta a misurare il loro ambiente rispetto agli standard e alle migliori pratiche del settore della sicurezza. Funziona raccogliendo eventi e dati da altri servizi AWS, come AWS Config GuardDuty, Amazon e AWS Firewall Manager. Questi eventi e dati vengono analizzati in base agli standard di sicurezza, come CIS AWS Foundations Benchmark. Le eccezioni vengono dichiarate come risultati nella console di AWS Security Hub. I nuovi risultati vengono inviati come eventi Amazon EventBridge .
2. Ascolta: EventBridge gli eventi vengono emessi da AWS Security Hub per ogni risultato creato o modificato dal servizio. Automated Security Response on AWS (ASR) implementa due EventBridge regole che consentono di individuare gli eventi generati da AWS Security Hub:
   - EventBridge Regola di azione personalizzata: ascolta gli eventi di azioni personalizzate emessi da AWS Security Hub CSPM quando l'azione personalizzata «Remediate with ASR» viene attivata da un utente. L'evento viene inoltrato all'Orchestrator per la correzione.
   - EventBridge Regola dei risultati: ascolta tutti gli eventi di ricerca, creazione o aggiornamento emessi da AWS Security Hub e AWS Security Hub CSPM. La regola inoltra questi eventi alla coda SQS di The SQS per Pre-Processor un'ulteriore elaborazione. Associa Pre-Processor ogni risultato alla correzione appropriata. Oltre ai risultati del controllo CSPM di AWS Security Hub, la soluzione può correggere i risultati di servizi di sicurezza AWS aggiuntivi: Amazon Inspector, Amazon e Amazon GuardDuty Macie. La soluzione elabora sia l'AWS Security Finding Format (ASFF) utilizzato da AWS Security Hub CSPM sia l'Open Cybersecurity Schema Framework (OCSF) utilizzato da AWS Security Hub v2.
3. Avvio: puoi avviare le correzioni manualmente o configurarle per l'esecuzione automatica. Per eseguire una correzione manualmente, puoi utilizzare l'interfaccia utente Web distribuita dalla soluzione o la funzionalità di azioni personalizzate in AWS Security Hub CSPM. Dopo accurati test in un ambiente non di produzione, puoi anche attivare correzioni automatiche. È possibile attivare le automazioni per le singole correzioni: non è necessario attivare le iniziazioni automatiche per

tutte le correzioni. Per configurare le correzioni in modo che vengano eseguite automaticamente, consulta la pagina Abilita le correzioni completamente automatiche. ???

4. Pre-remediate: nell'account amministratore, AWS Step Functions elabora l'evento di riparazione e lo prepara per la pianificazione.
5. Pianificazione: la soluzione richiama la funzione di pianificazione di AWS Lambda per inserire l'evento di riparazione nella tabella di stato di Amazon DynamoDB. https://aws.amazon.com/dynamodb
6. Orchestrate: nell'account amministratore, Step Functions utilizza ruoli AWS Identity and Access Management (IAM) multiaccount. Step Functions richiama la correzione nell'account membro contenente la risorsa che ha prodotto il risultato di sicurezza.
7. Remediate: un documento AWS Systems Manager Automation nell'account membro esegue l'azione necessaria per correggere il risultato sulla risorsa di destinazione, ad esempio disabilitare l'accesso pubblico a Lambda.

   Facoltativamente, puoi abilitare la funzionalità Action Log negli stack dei membri con il parametro. EnableCloudTrailForASRActionLog Questa funzione registra le azioni intraprese dalla soluzione nei tuoi account membri e le visualizza nella dashboard Amazon della soluzione. CloudWatch
8. (Facoltativo) Crea un ticket: se utilizzi il TicketGenFunctionName parametro per abilitare il ticketing nello stack di amministrazione, la soluzione richiama la funzione Lambda del generatore di ticket fornita. Questa funzione Lambda crea un ticket nel tuo servizio di biglietteria dopo che la correzione è stata eseguita con successo nell'account del Membro. Forniamo stack per l'integrazione con Jira e. ServiceNow
9. Notifica e registra: il playbook registra i risultati in un gruppo di CloudWatch log, aggiorna i risultati di AWS Security Hub e mantiene un audit trail delle azioni nelle note sui risultati. La soluzione quindi distribuisce e monitora i risultati tramite una pipeline di notifiche dedicata:
   a. Mettere in coda e inviare la notifica: Orchestrator invia il risultato della correzione a una coda di notifica Amazon Simple Queue Service (Amazon SQS). Una funzione Lambda del dispatcher di notifica consuma la coda e distribuisce il risultato tramite un argomento Amazon Simple Notification Service (Amazon SNS) gestito dalla soluzione. https://aws.amazon.com/sns/ Oltre all'argomento SNS gestito dalla soluzione, puoi creare configurazioni di notifica dall'interfaccia utente Web per inviare i risultati e le correzioni via e-mail, Slack, JIRA o un argomento SNS. ServiceNow Per ulteriori informazioni, consulta la sezione Configurazione delle notifiche. ???
   b. Monitora la distribuzione: gli CloudWatch allarmi della soluzione vengono pubblicati su un argomento relativo agli allarmi SNS e la CloudWatch dashboard ASR Amazon mostra lo stato delle procedure di correzione e notifica in modo da poter rilevare gli errori di consegna.

Considerazioni sulla progettazione di AWS Well-Architected

Questa soluzione è stata progettata con le migliori pratiche di AWS Well-Architected Framework che aiutano i clienti a progettare e gestire carichi di lavoro affidabili, sicuri, efficienti ed economici nel cloud. Questa sezione descrive come sono stati applicati i principi di progettazione e le best practice del Well-Architected Framework durante la creazione di questa soluzione.

Eccellenza operativa

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le best practice del pilastro dell'eccellenza operativa.

- Risorse definite come IaC che utilizzano. CloudFormation
- Correzioni implementate con le seguenti caratteristiche, ove possibile:
  - Idempotenza
  - Gestione e segnalazione degli errori
  - Registrazione dei log
  - Ripristino delle risorse a uno stato noto in caso di errore

Sicurezza

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le best practice del pilastro della sicurezza.

- IAM è utilizzato per l'autenticazione e l'autorizzazione.
- L'ambito delle autorizzazioni di ruolo è il più ristretto possibile, sebbene in molti casi questa soluzione richieda autorizzazioni wildcard per poter agire su qualsiasi risorsa.
- Per motivi di sicurezza, tutti i ruoli IAM distribuiti da questa soluzione utilizzano autorizzazioni con privilegi minimi limitate alle risorse specifiche che gestiscono.

Affidabilità

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'affidabilità. https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/welcome.html

- Security Hub continua a creare risultati se la causa alla base della scoperta non viene risolta con la correzione.
- I servizi serverless consentono alla soluzione di scalare in base alle esigenze.

Efficienza delle prestazioni

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le best practice del pilastro dell'efficienza delle prestazioni.

- Questa soluzione è stata progettata per essere una piattaforma da estendere senza dover implementare personalmente l'orchestrazione e le autorizzazioni.

Ottimizzazione dei costi

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le best practice del pilastro dell'ottimizzazione dei costi.

- I servizi serverless consentono di pagare solo ciò che si utilizza.
- Utilizza il livello gratuito per l'automazione SSM in ogni account

Sostenibilità

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro della sostenibilità.

- I servizi serverless consentono di aumentare o ridurre la scalabilità in base alle esigenze.

Dettagli dell'architettura

Questa sezione descrive i componenti e i servizi AWS che compongono questa soluzione e i dettagli dell'architettura su come questi componenti interagiscono.

Integrazione con AWS Security Hub

La distribuzione `automated-security-response-admin` dello stack crea l'integrazione con la funzionalità di azione personalizzata di AWS Security Hub CSPM. Quando gli utenti della console CSPM di AWS Security Hub scelgono Azioni > Remediate with ASR, i risultati selezionati vengono inviati a e attivano il flusso di lavoro di correzione. EventBridge

Cross-account le autorizzazioni e i runbook di AWS Systems Manager devono essere distribuiti a tutti gli account AWS Security Hub (amministratore e membro) utilizzando i modelli and. `automated-security-response-member.template` `automated-security-response-member-roles.template` CloudFormation Per ulteriori informazioni, consulta Playbooks. ??? Questo modello consente la correzione automatica nell'account di destinazione.

Gli utenti possono configurare correzioni completamente automatiche per controllo utilizzando Amazon DynamoDB. Questa opzione attiva la correzione completamente automatica dei risultati non appena vengono segnalati ad AWS Security Hub. Per impostazione predefinita, le iniziazioni automatiche sono disattivate. Questa opzione può essere modificata in qualsiasi momento dopo l'installazione modificando la tabella Remediation Configuration DynamoDB.

Cross-account bonifica

Automated Security Response on AWS utilizza ruoli tra più account per funzionare su account primari e secondari. Questi ruoli vengono distribuiti agli account dei membri durante l'installazione della soluzione. A ogni correzione viene assegnato un ruolo individuale. Al processo di riparazione nell'account principale viene concessa l'autorizzazione ad assumere il ruolo di correzione nell'account che richiede la correzione. La riparazione viene eseguita dai runbook di AWS Systems Manager in esecuzione nell'account che richiede la correzione.

Playbook

Una serie di soluzioni è raggruppata in un pacchetto chiamato playbook. I playbook vengono installati, aggiornati e rimossi utilizzando i modelli di questa soluzione. Per informazioni sulle

correzioni supportate in ogni playbook, consulta Playbooks (nella Guida per gli sviluppatori). Questa soluzione attualmente supporta i seguenti playbook:

- Security Control, una guida in linea con la funzionalità Consolidated control finding di AWS Security Hub, pubblicata il 23 febbraio 2023.

  > **Important**
  >
  > Quando i risultati di controllo consolidati sono abilitati in Security Hub, questo è l'unico playbook che dovrebbe essere abilitato nella soluzione.

- Benchmark Amazon Web Services Foundations del Center for Internet Security (CIS), versione 1.2.0, pubblicati il 18 maggio 2018.
- Benchmark del Center for Internet Security (CIS) Amazon Web Services Foundations, versione 1.4.0, pubblicati il 9 novembre 2022.
- Benchmark del Center for Internet Security (CIS) Amazon Web Services Foundations, versione 3.0.0, pubblicati il 13 maggio 2024.
- AWS Foundational Security Best Practices (FSBP) versione 1.0.0, pubblicata a marzo 2021.
- Payment Card Industry Data Security Standards (PCI-DSS) versione 3.2.1, pubblicata a maggio 2018.
- National Institute of Standards and Technology (NIST) versione 5.0.0, pubblicata nel novembre 2023.

Dopo aver implementato gli CloudFormation stack della soluzione, i playbook sono immediatamente pronti per l'uso: non è necessaria alcuna configurazione aggiuntiva per abilitare le correzioni agli standard di sicurezza sopra elencati.

Registrazione centralizzata

Risposta di sicurezza automatizzata sui log AWS a un singolo gruppo di CloudWatch log,. SO0111-ASR Questi registri contengono registrazioni dettagliate della soluzione per la risoluzione dei problemi e la gestione della soluzione.

Multi-service riparazione

Oltre ai risultati di controllo CSPM di AWS Security Hub (identificati da ID di controllo come `S3.1` o`IAM.7`), la soluzione può correggere i risultati di servizi di sicurezza AWS aggiuntivi. Questi risultati

sono classificati in base al nome del servizio, al tipo di risultato e al tipo di risorsa anziché in base a un ID di controllo Security Hub. Il preprocessore associa ogni servizio e tipo di ricerca alla correzione appropriata. Multi-service le correzioni utilizzano la stessa architettura runbook a due livelli, lo stesso flusso di inserimento e orchestrazione delle correzioni basate sul controllo. Configurali allo stesso modo tramite la tabella Remediation Configuration Amazon DynamoDB.

Questa versione supporta un tipo di ricerca per servizio:

Servizio	ID controllo	Tipi di risorse supportati	Correzione	È richiesto un follow-up manuale
Amazon Inspector	`Inspector.InstanceVulnerability`	Istanze EC2 gestite da AWS Systems Manager	Esegue il comando `AWS-RunPatchBaseline` Systems Manager per installare i pacchetti vulnerabili specifici identificati nella scoperta. La versione dell'agente di Systems Manager deve essere 2.0.834.0 o successiva.	No
Amazon GuardDuty	`GuardDuty.IAMUser`	Chiavi di accesso IAM	Contiene l'utente IAM potenzialmente compromesso disabilitandone le chiavi di accesso, rimuovendo l'accesso alla console e allegando una politica di negazione dell'accesso, utilizzando il runbook. AWS-managed `AWSSupport-ContainIAMPrincipal` La soluzione esegue il backup della configurazione originale in modo da poter ripristinare il contenimento dall'interfaccia utente Web.	Sì

Servizio	ID controllo	Tipi di risorse supportati	Correzione	È richiesto un follow-up manuale
Amazon Macie	`Macie.SensitiveDataS3Object`	Bucket S3 contenenti oggetti con dati sensibili	Abilita S3 Block Public Access sul bucket per impedire l'esposizione pubblica dei dati sensibili.	Sì

È richiesto un follow-up manuale

Le soluzioni correttive di Amazon GuardDuty e Amazon Macie sono una prima linea di difesa e non risolvono la situazione sottostante. Contengono o limitano l'esposizione della risorsa interessata, ma un team di sicurezza deve indagare e completare il follow-up specifico del servizio prima di risolvere il problema. La scoperta rimane visibile nella soluzione per quel follow-up.

PerchéGuardDuty.IAMUser, il contenimento può essere ripristinato dall'interfaccia utente Web. Se la correzione automatica è abilitata per il controllo, l'interfaccia utente Web avvisa quando si avvia un rollback che la soluzione potrebbe correggere nuovamente il risultato, in quanto il ripristino lascia il risultato idoneo per consentire alla soluzione di intervenire nuovamente. Disabilita la correzione automatica del controllo prima del rollback se desideri che il rollback persista.

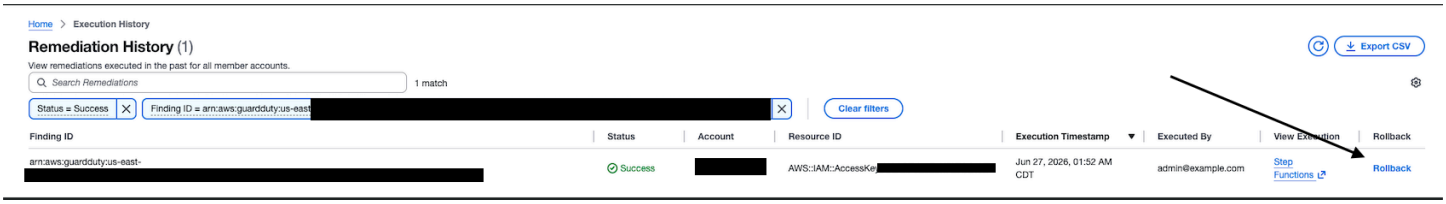
Poiché un rollback riporta la risorsa allo stato precedente alla riparazione (non conforme), il risultato sottostante rimane irrisolto. Re-enabling la correzione automatica del controllo quando il risultato è ancora irrisolto lo rende nuovamente idoneo, quindi la soluzione applica nuovamente la correzione la volta successiva che AWS Security Hub emette un evento per la scoperta. Mantieni la correzione automatica disattivata per il controllo finché non avrai esaminato e risolto il risultato sottostante.

GuardDuty.IAMUser credenziali temporanee

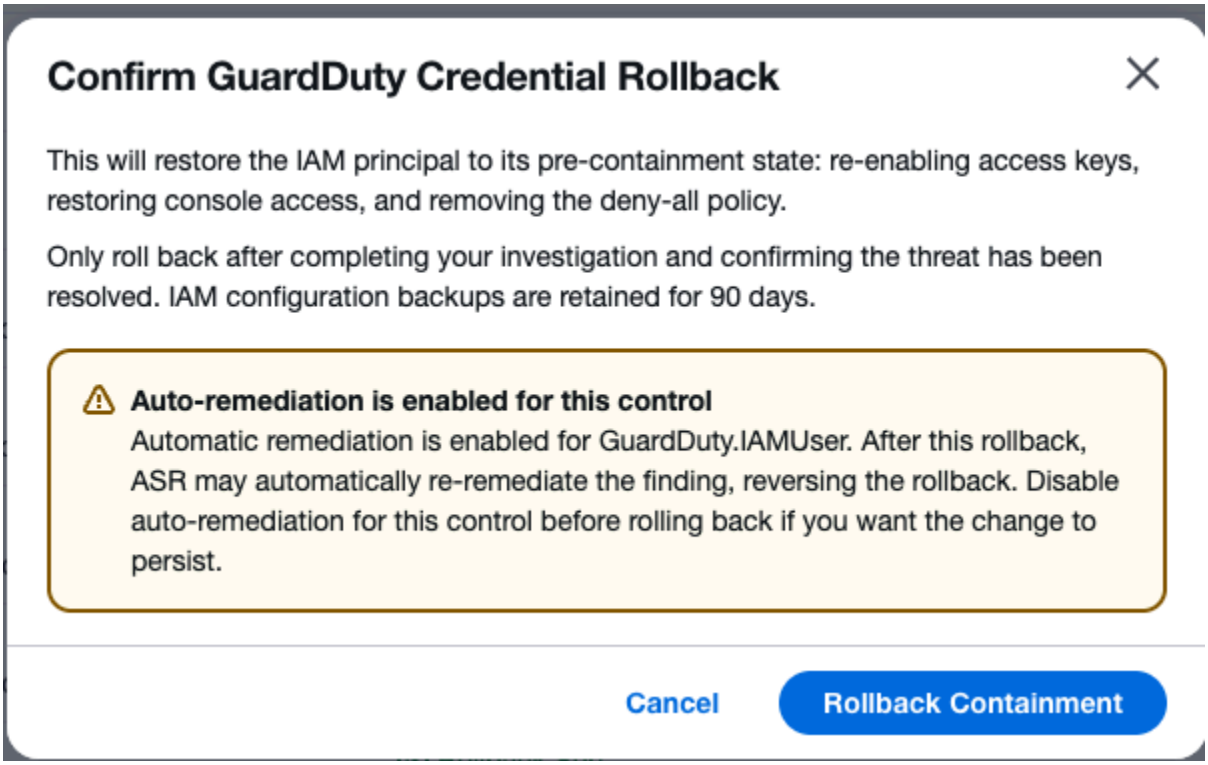
Il `AWSSupport-ContainIAMPrincipal` runbook contiene un utente IAM a lungo termine (l'ID della chiave di accesso inizia con`AKIA`). Un `GuardDuty.IAMUser` risultato il cui principale compromesso è una credenziale temporanea proveniente da una sessione federata o con un ruolo presunto (il cui ID della chiave di accesso inizia con`ASIA`) non deve

contenere alcun utente IAM, quindi ogni tentativo di correzione fallirebbe. La soluzione non corregge automaticamente questi risultati; li registra per garantirne la visibilità, ma non attiva mai la correzione. Analizza il ruolo o il provider di identità originario e revoca direttamente la sessione attiva.

GuardDuty.IAMUser pulsante di rollback nella cronologia delle riparazioni dell'interfaccia utente Web



GuardDuty.IAMUser avviso di rollback nell'interfaccia utente Web



Ricerca di formati

Security Hub rappresenta i risultati in due formati di schema e la soluzione li elabora entrambi:

- ASFF (AWS Security Finding Format): il formato utilizzato da AWS Security Hub CSPM (Classic). La soluzione elabora i risultati del controllo CSPM di AWS Security Hub in ASFF.

- OCSF (Open Cybersecurity Schema Framework): il formato utilizzato da AWS Security Hub v2. La soluzione elabora i risultati di Amazon Inspector GuardDuty, Amazon e Amazon Macie nel loro formato OCSF nativo.

Anziché forzare ogni risultato in un unico schema, la soluzione elabora ogni risultato nel formato emesso dal servizio sorgente. Le soluzioni correttive esistenti che utilizzano AWS Config continuano a funzionare senza modifiche in ASFF, mentre i risultati multiservizio vengono elaborati nel formato OCSF nativo.

Notifications

Questa soluzione utilizza un argomento Amazon Simple Notification Service (Amazon SNS) per pubblicare i risultati delle correzioni. Puoi utilizzare gli abbonamenti a questo argomento per estendere le funzionalità della soluzione. Ad esempio, è possibile inviare notifiche e-mail e aggiornare i ticket di assistenza.

- SO0111-ASR_Topic: utilizzato per inviare informazioni generali e messaggi di errore relativi alle correzioni eseguite.
- SO0111-ASR_ Alarm_Topic — Utilizzato per notificare quando viene attivato uno degli allarmi della soluzione, a indicare che la soluzione non funziona come previsto.

Servizi AWS inclusi in questa soluzione

La soluzione utilizza i seguenti servizi. I servizi principali sono necessari per utilizzare la soluzione e i servizi di supporto collegano i servizi principali.

Servizio AWS	Description
Amazon EventBridge	Nucleo. EventBridge le regole vengono utilizzate per ascoltare e attivare gli eventi emessi da AWS Security Hub e AWS Security Hub CSPM.
AWS IAM	Nucleo. Implementa molti ruoli per consentire correzioni su diverse risorse.

Servizio AWS	Description
AWS Lambda	Nucleo. Implementa più funzioni Lambda utilizzate dall'orchestrator Step Functions per risolvere i problemi. Funge da backend per l'interfaccia utente Web della soluzione integrata con API Gateway.
AWS Security Hub	Nucleo. Fornisce ai clienti una visione completa del loro stato di sicurezza AWS.
AWS Step Functions	Nucleo. Implementa un orchestrator che richiamerà i documenti di correzione con le chiamate API di AWS Systems Manager.
AWS Systems Manager	Nucleo. Distribuisce i documenti di automazione di System Manager che contengono la logica di correzione che deve essere eseguita dalla soluzione. Utilizza Parameter Store per mantenere i metadati e le impostazioni di configurazione della soluzione.
Amazon DynamoDB	Nucleo. Memorizza l'ultima correzione eseguita in ogni account e regione per ottimizzare la pianificazione delle correzioni. Memorizza i risultati generati da AWS Security Hub e AWS Security Hub CSPM. Memorizza i metadati di riparazione e configurazione della soluzione. Memorizza i dati per gli utenti che accedono all'interfaccia utente Web della soluzione.

Servizio AWS	Description
AWS CloudTrail	Supporto. Registra le modifiche apportate dalla soluzione alle risorse AWS e le visualizza su un CloudWatch pannello di controllo.
Amazon CloudWatch	Supporto. Distribuisce gruppi di log che i diversi playbook utilizzeranno per registrare i risultati . Raccoglie le metriche da visualizzare su una dashboard personalizzata con allarmi.
Amazon Simple Notification Service	Supporto. Distribuisce argomenti SNS che ricevono una notifica una volta completata la correzione.
Amazon SQS	Supporto. Aiuta a pianificare le correzioni in modo che la soluzione possa eseguirle in parallelo. Effettua il buffering delle esecuzioni Lambda utilizzando Lambda Mappings. EventSource
AWS Key Management Service	Supporto. Utilizzato per crittografare i dati per le correzioni.
AWS Config	Supporto. Registra tutte le risorse da utilizzare con AWS Security Hub.
Amazon Inspector	Supporto. La soluzione acquisisce i `Inspector.InstanceVulnerability` risultati di Amazon Inspector e corregge le istanze Amazon EC2 interessate.
Amazon GuardDuty	Supporto. La soluzione acquisisce GuardDuty `GuardDuty.IAMUser` i risultati di Amazon e contiene il principale IAM interessato.

Servizio AWS	Description
Amazon Macie	Supporto. La soluzione acquisisce i `Macie.SensitiveDataS3Object` risultati di Amazon Macie e blocca l'accesso pubblico al bucket Amazon S3 interessato.
Amazon S3	Supporto. Memorizza la cronologia delle riparazioni e i dati di registro esportati. Ospita l'interfaccia utente Web come Single-page applicazione (SPA) della soluzione.
Amazon CloudFront	Supporto. Fornisce l'interfaccia utente Web della soluzione
Gateway Amazon API	Supporto. Crea l'API REST della soluzione per supportare l'interfaccia utente.
AWS WAF	Supporto. Protegge l'interfaccia utente Web della soluzione.
Amazon Cognito	Supporto. Utilizzato per autenticare e autorizzare l'accesso all'interfaccia utente Web della soluzione.

Pianifica la tua implementazione

Questa sezione descrive i costi, la sicurezza della rete, le regioni AWS supportate, le quote e altre considerazioni prima di distribuire la soluzione.

Nozioni di base

Tempo di implementazione: circa 30 minuti per account.

Consigliamo di adottare la soluzione in più fasi anziché abilitare la correzione automatica ovunque e contemporaneamente. Con un approccio graduale, acquisirete fiducia in ogni correzione rispetto al vostro ambiente prima che la soluzione agisca in base ai risultati senza una revisione umana.

Utilizzate innanzitutto un ambiente non di produzione

Prima di abilitare la correzione completamente automatica in produzione, convalida i controlli che intendi automatizzare in un account e in un'area non di produzione. Riproduci il risultato su una risorsa disponibile, esegui la correzione e conferma il risultato. Questo ti offre un luogo sicuro in cui sperimentare nuovi controlli e filtri senza influire sui carichi di lavoro di produzione.

Cammina, poi corri

1. Osserva. Implementa la soluzione ed esamina i risultati che arrivano nell'interfaccia utente Web. In una nuova distribuzione, la correzione automatica è disattivata per impostazione predefinita, quindi nessuna correzione viene eseguita automaticamente in questa fase. Se invece si esegue l'aggiornamento da una versione ASR precedente, tutti i controlli configurati per la correzione automatica rimangono abilitati dopo l'aggiornamento, quindi le correzioni potrebbero essere eseguite automaticamente. In tal caso, consulta la pagina Controlli (o la tabella di configurazione della riparazione) per confermare quali controlli sono abilitati prima di procedere. Utilizza questa fase per verificare che i risultati degli account dei membri e delle regioni vengano aggregati nell'account amministratore e vengano visualizzati nella soluzione.
2. Correggi su richiesta. Esegui le correzioni manualmente dall'interfaccia utente Web o dall'azione personalizzata CSPM di AWS Security Hub, su singoli risultati. Esamina il risultato della correzione e la risorsa interessata prima di procedere. Se una correzione supporta il rollback, è possibile ripristinare la risorsa allo stato precedente alla riparazione dall'interfaccia utente Web. Con la correzione su richiesta, è possibile convalidare il comportamento di un controllo su risorse reali senza eseguire azioni automatiche.

3. Automatizza in modo selettivo. Quando sei sicuro del comportamento di un controllo, abilita una correzione completamente automatica per quel controllo. Abilita un controllo alla volta. Utilizza i filtri per limitare gli account, le unità organizzative e i tag delle risorse su cui agisce la soluzione. Per i passaggi, consulta Gestire la correzione automatica.

Costo

Sei responsabile del costo dei servizi AWS utilizzati per eseguire questa soluzione.

A partire da questa revisione, i costi mensili stimati sono:

- Implementazione ridotta (10 account, 1 regione - Stati Uniti) East/N Virginia): circa 14,70 USD per 300 remediations/month
- Implementazione media (100 account, 1 regione: Stati Uniti. East/N Virginia): circa 106,40 USD per 3.000 remediations/month
- Implementazione su larga scala (1.000 account, 10 regioni): circa 7.360,00 USD per 30.000 remediations/month

> **Important**
>
> I prezzi sono soggetti a modifiche. Per i dettagli completi, consulta la pagina dei prezzi di ciascun servizio AWS utilizzato in questa soluzione.

> **Note**
>
> Molti servizi AWS includono un piano gratuito, un importo base del servizio che i clienti possono utilizzare gratuitamente. I costi effettivi possono essere superiori o inferiori agli esempi di prezzi forniti.

Ti consigliamo di creare un budget tramite AWS Cost Explorer per aiutare a gestire i costi. I prezzi sono soggetti a modifiche. Per i dettagli completi, consulta la pagina web dei prezzi per ogni servizio AWS utilizzato in questa soluzione.

Esempio di tabella dei costi

Il costo totale per l'esecuzione di questa soluzione dipende dai seguenti fattori:

- Il numero di account membri di AWS Security Hub
- Il numero di correzioni attive richiamate automaticamente
- La frequenza delle riparazioni

Questa soluzione utilizza i seguenti componenti AWS, che comportano un costo in base alla configurazione. Vengono forniti esempi di prezzi per organizzazioni di piccole, medie e grandi dimensioni.

Servizio	Piano gratuito	Prezzi [USD]
AWS Systems Manager Automation: numero di passaggi	Nessun livello gratuito	Ogni passaggio base ha un costo di 0,002 USD per passaggio. Per le automazioni con più account, tutti i passaggi, compresi quelli eseguiti in qualsiasi account figlio, vengono conteggiati solo nell'account di origine.
AWS Systems Manager Automation - Durata delle fasi	Nessun livello gratuito	Ogni fase di `aws:executeScript` azione viene addebitata a 0,00003 USD per ogni secondo.
AWS Systems Manager Automation - Storage	Nessun livello gratuito	0,046 USD per GB al mese
AWS Systems Manager Automation - Trasferimento dati	Nessun livello gratuito	0,900 USD per GB trasferito (per più account o fuori regione)
AWS Security Hub CSPM - Controlli di sicurezza	Nessun livello gratuito	I primi 100.000 dollari checks/account/Region/month costa 0,0010 USD per assegno

Servizio	Piano gratuito	Prezzi [USD]
		I successivi 400.000 dollari checks/account/Region/month costano 0,0008 USD per assegno Oltre 500.000 USD checks/account/Region/month costa 0,0005 USD per assegno
AWS Security Hub CSPM - Individuazione degli eventi di ingestione	I primi 10.000€ events/account sono gratuiti. Region/month Individuazione degli eventi di ingestione associati ai controlli di sicurezza di Security Hub.	Oltre 10.000 dollari events/account/Region/month costa 0,00003 USD per evento
Amazon - Metriche CloudWatch	Metriche di monitoraggio di base (con una frequenza di 5 minuti) 10 Metriche di monitoraggio dettagliate (con una frequenza di 1 minuto) 1 1 milione di richieste API (non applicabile a GetMetric Data, GetInsightRuleReport e) GetMetricWidgetImage	Le prime 10.000 metriche costano 0,30 USD metric/month Le successive 240.000 metriche costano 0,10 USD metric/month Le prossime 750.000 metriche costano 0,05 USD metric/month Oltre 1.000.000 di metriche costano 0,02 USD metric/month Le chiamate API costano 0,01 USD ogni 1.000 richieste
Amazon CloudWatch - Pannello di controllo	3 dashboard per un massimo di 50 metriche al mese	3,00 USD per dashboard al mese

Servizio	Piano gratuito	Prezzi [USD]
Amazon CloudWatch - Allarmi	10 parametri relativi agli allarmi (non applicabili agli allarmi ad alta risoluzione)	La risoluzione standard (60 sec) costa 0,10 USD per ogni metrica di allarme L'alta risoluzione (10 sec) costa 0,30 USD per metrica di allarme Il rilevamento delle anomalie a risoluzione standard costa 0,30 USD per allarme Il rilevamento delle anomalie ad alta risoluzione costa 0,90 USD per allarme Il costo del composito è di 0,50 USD per allarme
Amazon CloudWatch - Raccolta di log	5 GB di dati (inserimento, archiviazione e dati scansionati tramite query Logs Insights)	0,50 USD per GB
Amazon CloudWatch - Archiviazione dei log	5 GB di dati (inserimento, archiviazione e dati scansionati tramite query Logs Insights)	0,005 USD per GB di dati scansionati
AWS Lambda - Richieste	1 milione di richieste gratuite al mese	0,20 USD per 1 milione di richieste

Servizio	Piano gratuito	Prezzi [USD]
AWS Lambda - Durata	400.000 GB-seconds di tempo di calcolo al mese	$0,0000166667 per ogni. GB-second Il prezzo di Duration dipende dalla quantità di memoria allocata alla funzione. È possibile allocare qualsiasi quantità di memoria alla funzione compresa tra 128 MB e 10.240 MB, con incrementi di 1 MB.
AWS Step Functions - Transizioni di stato	4.000 transizioni di stato gratuite al mese	0,025 USD per 1.000 transizioni di stato successive
Amazon EventBridge	Tutti gli eventi di modifica dello stato pubblicati dai servizi AWS sono gratuiti	Gli eventi personalizzati costano 1 dollaro. 00/million eventi personalizzati pubblicati Third-party Gli eventi (SaaS) costano $1. 00/million eventi pubblicati Cross-account gli eventi costano $1. 00/million eventi tra account inviati
Amazon SNS	Il primo milione di richieste Amazon SNS al mese sono gratuite	0,50 USD per 1 milione di richieste successive
Amazon SQS	Il primo milione di richieste Amazon SQS al mese sono gratuite	0,40 USD per 1-100 miliardi di richieste successive

Servizio	Piano gratuito	Prezzi [USD]
Amazon DynamoDB	I primi 25 GB di spazio di archiviazione sono gratuiti	0,25 USD per GB al mese per lo spazio di archiviazione oltre il livello gratuito. On-demand il prezzo della richiesta è di 1,25 USD per 1 milione di unità di richiesta di scrittura e 0,25 USD per 1 milione di unità di richiesta di lettura. La soluzione fornisce diverse tabelle nell'account amministratore (risultati, cronologia delle riparazioni, configurazione delle riparazioni, filtri delle risorse, configurazione delle notifiche, batch di notifiche, pianificazione e mappatura degli account utente). Lo spazio di archiviazione per le tabelle Findings e Remediation History aumenta con il numero di risultati aggregati tra i tuoi account e le aree geografiche.

Servizio	Piano gratuito	Prezzi [USD]
AWS Key Management Service	20.000 requests/month	1,00 USD per 1 chiave AWS KMS. 0,03 USD per 10.000 richieste API. Per le chiavi AWS KMS che ruotano automaticamente o su richiesta, la prima e la seconda rotazione della chiave aggiungono $ (proporzionalmente all'ora) di costo. 1/month Nota: questa soluzione include ottimizzazioni della cache di AWS KMS (chiavi S3 Bucket, riutilizzo delle chiavi di dati SQS di 60 minuti, caching di Secrets Manager di 5 minuti) che riducono le chiamate API AWS KMS di circa il 70%.
Amazon Cognito	Nel livello Essentials, i primi 10.000 utenti attivi mensili sono gratuiti. Nota: questo livello gratuito è di 50 utenti attivi mensili quando gli utenti si autentica no tramite IdP esterno (). SAML/OIDC	0,015 USD per utente attivo mensile superiore a 10.000 utenti.

Servizio	Piano gratuito	Prezzi [USD]
Amazon CloudFront	Il piano gratuito include 1 TB di trasferimento dati in uscita e 10.000.000 di richieste HTTP o HTTPS al mese.	(US/Canada/Mexico) I primi 9 TB costano 0,085 USD al mese. I successivi 40 TB costano 0,080 USD al mese. 0,0075 USD per richiesta HTTP. 0,0100 USD per richiesta HTTPS.
Amazon S3	Nessun livello gratuito	I primi 50 TB costano 0,023 USD per GB al mese. 0,005 USD per 1.000 richieste PUT, COPY, POST, LIST. 0,0004 USD per 1.000 richieste GET, SELECT e tutte le altre richieste.
Gateway Amazon API	1 milione di chiamate API REST nei primi 12 mesi di utilizzo.	3,50 dollari per milione per i primi 333 milioni di chiamate API.
AWS Secrets Manager	Prova gratuita di 30 giorni per ogni segreto.	0,40 USD per codice segreto al mese. 0,05 USD per 10.000 chiamate API. Utilizzato per archiviare le credenziali per Slack, JIRA e i canali di ServiceNow notifica e bigliette ria; un segreto per canale configurato.

Servizio	Piano gratuito	Prezzi [USD]
AWS WAF	Nessun livello gratuito	5,00 USD per ACL web al mese. 1,00 USD per regola al mese. 0,60 USD per 1 milione di richieste. Distribui to per proteggere l'API Web UI quando l'interfaccia utente Web è abilitata, con 10 regole (7 gruppi di regole gestite da AWS più 3 regole basate sulla tariffa per la limitazione della velocità per utente e per IP). Il gruppo di regole AWS Managed Bot Control aggiunge prezzi per la mitigazione intelligente delle minacce pari a 10,00 USD al mese più 1,00 USD per 1 milione di richieste.
AWS CloudTrail	La prima copia degli eventi di gestione è gratuita.	2,00 USD per 100.000 eventi di gestione. Gli eventi relativi ai dati costano 0,10 USD per 100.000 eventi. Si verifica solo quando si abilita il registro delle azioni con il parametro. EnableCloudTrailForASRActio nLog

Ottimizzazione dei costi di AWS KMS

A partire dalla versione 3.1.0, questa soluzione include ottimizzazioni di caching di AWS KMS che riducono i costi delle operazioni crittografiche di circa il 70%

- S3 Bucket Keys: riduce le chiamate AWS KMS per le operazioni di crittografia S3 GenerateDataKey

- SQS Data Key Reuse: periodo di cache di 60 minuti per la crittografia dei messaggi
- Secrets Manager Caching: TTL in 5 minuti nelle funzioni Lambda

Impatto sulle prestazioni: queste ottimizzazioni migliorano la latenza di 10-15 ms per le operazioni S3 e i flussi di lavoro completi, riducendo al contempo i costi, senza alcuna riduzione del throughput.

Esempi di prezzi (mensili)

> **Note**
>
> Le cifre di Amazon DynamoDB negli esempi seguenti rappresentano le tabelle Findings and Remediation History, che dominano lo storage. Le altre tabelle della soluzione (Remediation Configuration, Resource Filters, Notification Configuration, Notification Batches, Scheduling e User Account Mapping) contengono dati trascurabili e vengono omesse per motivi di chiarezza. Gli esempi presuppongono inoltre che tu non abbia configurato Slack, JIRA o i ServiceNow canali; ogni canale configurato aggiunge un segreto di AWS Secrets Manager (vedi la precedente tabella dei componenti). Le voci di AWS Lambda e Amazon SNS includono la pipeline di notifica (le funzioni di notification-dispatcher e fanout Lambda per canale e gli argomenti SNS per configurazione su cui pubblicano); ai volumi di richiesta qui modellati, aggiungono ben meno di 0,01$ a Lambda (0,20$ per 1 milione di richieste) e SNS (0,50$ per 1 milione di richieste). AWS WAF (e il relativo addebito per la mitigazione intelligente delle minacce di Bot Control) appare solo negli UI-enabled esempi Web, poiché l' WAF-protected API Gateway viene distribuito solo quando l'interfaccia utente Web è abilitata.

Esempio 1:300 correzioni al mese

- 10 account, 1 regione
- 30 riparazioni al mese account/Region
- 500 risultati di Security Hub elaborati al mese account/Region
- Interfaccia utente Web disattivata
- Registro azioni disabilitato
- Costo totale $14,70 al mese

Servizio	Presupposti	Spese mensili [USD]
Automazione di AWS Systems Manager	Fasi: ~4 passaggi * 300 riparazioni * 0,002 USD = 2,40 USD Durata: 10 secondi * 300 riparazioni * 0,00003 USD = 0,09 USD	2,49$
Centrale di sicurezza AWS	Nessun servizio fatturabile utilizzato	0 USD
Amazon Logs CloudWatch	0,50 USD per GB	< 0,01 USD
AWS Lambda - Richieste	300 correzioni * 7 richieste = 2.100 richieste 5.000 risultati * 1 richiesta = 5.000 richieste 0,20 USD/1.000.000 di richieste = 0,0000002 USD per richiesta	0,00142 USD
AWS Lambda - Durata	(512 MB di memoria) 4.000 ms * 300 riparazioni * 0,0000000083 USD = 0,00996 USD 449 ms * 5.000 risultati * $0.0000000083 = $.0186	0,029$
AWS Step Functions	19 transizioni di stato * 300 riparazioni = 5.700 0,025 USD * (5.000) transizio ni di stato = 0,14 700/1 USD	0,14 USD

Servizio	Presupposti	Spese mensili [USD]
Regole di Amazon EventBridge	Nessun costo per le regole	0 USD
AWS Key Management Service	1 chiave * 10 account * 1 regione * $1 = $10 (richieste Encrypt/Decrypt API) (300 correzioni * 2 richieste) + (5.000 risultati * 4 richieste) = 20.600 richieste Con la memorizzazione nella cache di AWS KMS: 20.600 * 0,30 = 6.180 richieste 0,03 USD per 10.000 richieste ⇒ 0,03 USD * (6.180/10.000) = 0,02 USD	10,02 USD
Amazon DynamoDB	2,00 USD * 1.000.000 in lettura e scrittura = 2,00 USD (Tabella dei risultati) 15 MB * 10 account * 1 regione = 150 MB (Tabella storica) 10 MB * 10 account * 1 regione = 100 MB 0,25 USD per GB-month * 0,25 GB = 0,0625 USD	2,0625 USD
Amazon SQS	0,40 USD * 1.000.000 di richieste = 0,40 USD	0,40 USD
Amazon SNS	0,50 USD * (600/1.000.000 di notifiche) = 0,0003 USD	0,0003 USD

Servizio	Presupposti	Spese mensili [USD]
Amazon CloudWatch - Metriche	(Metriche avanzate disattivate) 0,30 USD * 7 metriche personalizzate = 2,10 USD 0,01 USD * (300 chiamate API per metriche put/1.000) = 0,003 USD	2,10 USD
Amazon CloudWatch - Dashboard	$3,00 * 1 pannello di controllo = $3,00	3,00 USD
Amazon CloudWatch - Allarmi	(Metriche avanzate disattivate) 0,10 USD * 4 allarmi = 0,40 USD	0,40 USD
Amazon CloudWatch - Tracce X-Ray	300 correzioni * 7 richieste = 2.100 chiamate Lambda 5.000 risultati * 1 richiesta = 5.000 richiami Lambda 0,000005 USD per traccia * 7.100 tracce = 0,0355 USD	0,0355$
Totale		14,70$

Esempio 2:300 correzioni al mese (interfaccia utente Web abilitata)

- 10 account, 1 regione
- 30 riparazioni al mese account/Region
- 5.000 risultati di Security Hub elaborati al mese account/Region
- Interfaccia utente Web abilitata
- Registro azioni disabilitato
- Costo totale 49,31$ al mese

Servizio	Presupposti	Spese mensili [USD]
Automazione di AWS Systems Manager	Fasi: ~4 passaggi * 300 riparazioni * 0,002 USD = 2,40 USD Durata: 10 secondi * 300 riparazioni * 0,00003 USD = 0,09 USD	2,49$
Centrale di sicurezza AWS	Nessun servizio fatturabile utilizzato	0 USD
Amazon Logs CloudWatch	0,50 USD per GB	< 0,01 USD
AWS Lambda - Richieste	300 correzioni * 7 richieste = 2.100 richieste 5.000 risultati * 1 richiesta = 5.000 richieste 0,20 USD/1.000.000 di richieste = 0,0000002 USD per richiesta	0,00142 USD
AWS Lambda - Durata	(512 MB di memoria) 4.000 ms * 300 riparazioni * 0,0000000083 USD = 0,00996 USD 449 ms * 5.000 risultati * $0.0000000083 = $.0186	0,029$
AWS Step Functions	19 transizioni di stato * 300 riparazioni = 5.700 0,025 USD * (5.000) transizio ni di stato = 0,14 700/1 USD	0,14 USD

Servizio	Presupposti	Spese mensili [USD]
Regole di Amazon EventBridge	Nessun costo per le regole	0 USD
AWS Key Management Service	1 chiave * 10 account * 1 regione * $1 = $10 (richieste Encrypt/Decrypt API) (300 correzioni * 2 richieste) + (5.000 risultati * 4 richieste) = 20.600 richieste Con la memorizzazione nella cache di AWS KMS: 20.600 * 0,30 = 6.180 richieste 0,03 USD per 10.000 richieste ⇒ 0,03 USD * (6.180/10.000) = 0,02 USD	10,02 USD
Amazon DynamoDB	2,00 USD * 1.000.000 in lettura e scrittura = 2,00 USD (Tabella dei risultati) 15 MB * 10 account * 1 regione = 150 MB (Tabella della cronologia) 10 MB * 10 account * 1 regione = 100 MB 0,25 USD per GB-month * 0,25 GB = 0,0625 USD	2,0625 USD
Amazon SQS	0,40 USD * 1.000.000 di richieste = 0,40 USD	0,40 USD

Servizio	Presupposti	Spese mensili [USD]
Amazon SNS	0,50 USD * (600/1.000.000 di notifiche) = 0,0003 USD	0,0003 USD
Amazon CloudWatch - Metriche	(Metriche avanzate disattivate) 0,30 USD * 7 metriche personalizzate = 2,10 USD 0,01 USD * (300 chiamate API per metriche put/1.000) = 0,003 USD	2,10 USD
Amazon CloudWatch - Dashboard	$3,00 * 1 pannello di controllo = $3,00	3,00 USD
Amazon CloudWatch - Allarmi	(Metriche avanzate disattivate) 0,10 USD * 4 allarmi = 0,40 USD	0,40 USD
Amazon CloudWatch - Tracce X-Ray	300 correzioni * 7 richieste = 2.100 chiamate Lambda 5.000 risultati * 1 richiesta = 5.000 richiami Lambda 0,000005 USD per traccia * 7.100 tracce = 0,0355 USD	0,0355$
Amazon Cognito	(Livello Essentials) 500 utenti attivi mensili	0 USD

Servizio	Presupposti	Spese mensili [USD]
Amazon CloudFront	Trasferimento dati regionale dall'origine (per GB) = 0,020 USD Trasferimento dati regionale verso Internet (per GB) = 0,085 USD Richiedi il prezzo per tutti i metodi HTTP (per 10.000) = 0,0075 USD	0,1125 USD
Simple Storage Service (Amazon S3)	(Hosting dell'interfaccia utente) 0,023 USD per GB * 0,002 GB = 0,000046 USD (Esportazione della cronologia) 0,023 USD per GB * 0,50 GB = 0,0125 USD 0,0004 USD per 1.000 richieste GET	0,0125 USD

Servizio	Presupposti	Spese mensili [USD]
AWS WAF	1 Web ACL = 5,00 USD al mese 10 regole * 1,00 USD per regola = 10,00 USD (7 gruppi di regole gestite da AWS + 3 regole basate sulla tariffa) Attenuazione intelligente delle minacce con Bot Control = 10,00 USD al mese (più 1,00 USD per 1 milione di richieste e 0,60 USD per 1 milione di richieste WAF, entrambi irrisori se si considerano i volumi di richieste dell'interfaccia utente Web)	25,00 USD
Gateway Amazon API	3,50 USD per milione di chiamate API REST	3,50 USD
Totale		49,31$

Esempio 3:3.000 riparazioni al mese

- 100 account, 1 regione
- 30 riparazioni al mese account/Region
- 500 risultati di Security Hub elaborati al mese account/Region
- Interfaccia utente Web disattivata
- Registro azioni disabilitato
- Costo totale 106,49$ al mese

Servizio	Presupposti	Spese mensili [USD]
Automazione di AWS Systems Manager	Fasi: ~4 passaggi * 3.000 riparazioni * 0,002 USD = 24,00 USD Durata: 10 secondi * 3.000 riparazioni * 0,00003 USD = 0,90 USD	24,90$
Centrale di sicurezza AWS	Nessun servizio fatturabile utilizzato	0 USD
Amazon Logs CloudWatch	0,50 USD per GB	< 0,01 USD
AWS Lambda - Richieste	3.000 correzioni * 7 richieste = 21.000 richieste 50.000 risultati * 1 richiesta = 50.000 richieste 0,20 USD/1.000.000 di richieste = 0,0000002 USD per richiesta	0,01 USD
AWS Lambda - Durata	(512 MB di memoria) 4.000 ms * 3.000 riparazioni * 0,0000000083 USD = 0,0996 USD 449 ms * 50.000 risultati * 0,0000000083 USD = 0,186 USD	0,29$
AWS Step Functions	19 transizioni di stato * 3.000 riparazioni = 57.000	1,425 USD

Servizio	Presupposti	Spese mensili [USD]
	0,025 USD * (57.000) transizioni di stato = 1,425 USD 000/1	
Regole di Amazon EventBridge	Nessun costo per le regole	0 USD
AWS Key Management Service	1 chiave * 100 account * 1 regione * $1 = $100 (richieste Encrypt/Decrypt API) (3.000 correzioni * 2 richieste) + (50.000 risultati * 4 richieste) = 206.000 richieste Con la memorizzazione nella cache di AWS KMS: 206.000 * 0,30 = 61.800 richieste 0,03 USD per 10.000 richieste ⇒ 0,03 USD * (61.800/10.000) = 0,185 USD	100,185 USD
Amazon DynamoDB	2,00 USD * 1.000.000 in lettura e scrittura = 2,00 USD (Tabella dei risultati) 15 MB * 100 account * 1 regione = 1.500 MB (Tabella della cronologia) 10 MB * 100 account * 1 regione = 1.000 MB 0,25 USD per * 2,5 GB = 0,625 USD GB-month	2,625 USD

Servizio	Presupposti	Spese mensili [USD]
Amazon SQS	0,40 USD * 1.000.000 di richieste = 0,40 USD	0,40 USD
Amazon SNS	0,50 USD * 1.000.000 di notifiche = 0,50 USD	0,50 USD
Amazon CloudWatch - Metriche	(Metriche avanzate disattivate) 0,30 USD * 7 metriche personalizzate = 2,10 USD 0,01 USD * (3000/1.000) chiamate API put metrics = 0,03 USD	2,13 USD
Amazon CloudWatch - Dashboard	$3,00 * 1 pannello di controllo = $3,00	3,00 USD
Amazon CloudWatch - Allarmi	0,10 USD * 4 allarmi = 0,40 USD	0,40 USD
Amazon CloudWatch - Tracce X-Ray	3.000 correzioni * 7 richieste = 21.000 chiamate Lambda 50.000 risultati * 1 richiesta = 50.000 richiami Lambda 0,000005 USD per traccia * 71.000 tracce = 0,355 USD	0,355 USD
Totale		106,49$

Esempio 4:30.000 riparazioni al mese

- 1.000 account, 10 regioni
- 30 riparazioni al mese account/Region
- 500 risultati di Security Hub elaborati al mese account/Region

- Interfaccia utente Web disattivata
- Registro azioni disabilitato
- Costo totale 7.360,00$ al mese

Servizio	Presupposti	Spese mensili [USD]
Automazione di AWS Systems Manager	Fasi: ~4 passaggi * 30.000 riparazioni * 0,002 USD = 240,00 USD Durata: 10 secondi * 30.000 riparazioni * 0,00003 USD = 9,00 USD	249,00$
Centrale di sicurezza AWS	Nessun servizio fatturabile utilizzato	0 USD
Amazon Logs CloudWatch	0,50 USD per GB	< 0,01 USD
AWS Lambda - Richieste	30.000 correzioni * 7 richieste = 210.000 richieste 5.000.000 di risultati * 1 richiesta = 5.000.000 di richieste 0,20 USD/1.000.000 di richieste = 0,0000002 USD per richiesta	1,042 USD
AWS Lambda - Durata	(512 MB di memoria) 4.000 ms * 30.000 riparazioni * 0,0000000083 USD = 0,996 USD	19,63$

Servizio	Presupposti	Spese mensili [USD]
	449 ms * 5.000.000 di risultati * 0,0000000083 USD = 18,63 USD	
AWS Step Functions	19 transizioni di stato * 30.000 riparazioni = 570.000 0,025 USD * (570.000) transizioni di stato = 14,25 USD 000/1	14,25 USD
Regole di Amazon EventBridge	Nessun costo per le regole	0 USD
AWS Key Management Service	(1 chiave) $1 * 1.000 account * 10 regioni = 10.000$ (richieste Encrypt/Decrypt API) (30.000 correzioni * 2 richieste) + (5.000.000 di risultati * 4 richieste) = 20.060.000 richieste Con la memorizzazione nella cache di AWS KMS: 20.060.000 * 0,30 = 6.018.000 richieste 0,03 USD per 10.000 richieste ⇒ 0,03 USD * (6.018.00 0/10.000) = 18,05 USD	10.018,05 USD

Servizio	Presupposti	Spese mensili [USD]
Amazon DynamoDB	2,00$ * (10.000.000 in lettura e scrittura/1.000.000) = 20,00$ (Tabella dei risultati) 15 MB * 1000 account * 10 regioni = 150 GB (Tabella della cronologia) 10 MB * 1000 account * 10 regioni = 100 GB 0,25 USD per GB-month * 250 GB = 62,50 USD	82,50 USD
Amazon SQS	0,40 USD * (5.060.000 richieste/1.000.000) = 2.024 USD	2,024 USD
Amazon SNS	0,000005 USD * 1.000.000 di notifiche = 0,50 USD	0,50 USD
Amazon CloudWatch - Metriche	(Metriche avanzate disattivate) 0,30 USD * 7 metriche personalizzate = 2,10 USD 0,01 USD * (30.000/1.000) chiamate API put metrics = 0,30 USD	2,40 USD
Amazon CloudWatch - Dashboard	$3,00 * 1 pannello di controllo = $3,00	3,00 USD
Amazon CloudWatch - Allarmi	(Metriche avanzate disattivate) 0,10 USD * 4 allarmi = 0,40 USD	0,40 USD

Servizio	Presupposti	Spese mensili [USD]
Amazon CloudWatch - Tracce X-Ray	30.000 correzioni * 7 richieste = 210.000 chiamate Lambda 5.000.000 di risultati * 1 richiesta = 5.000.000 di richiami Lambda 0,000005 USD per traccia * 5.210.000 tracce = 26,05 USD	26,05$
Totale		7.360,00$

Esempio 5:30.000 correzioni al mese (interfaccia utente Web abilitata)

- 1.000 account, 10 regioni
- 30 riparazioni al mese account/Region
- 500 risultati di Security Hub elaborati al mese account/Region
- Interfaccia utente Web abilitata
- Registro azioni disabilitato
- Costo totale 7.393,10$ al mese

Servizio	Presupposti	Spese mensili [USD]
Automazione di AWS Systems Manager	Fasi: ~4 passaggi * 30.000 riparazioni * 0,002 USD = 240,00 USD Durata: 10 secondi * 30.000 riparazioni * 0,00003 USD = 9,00 USD	249,00$
Centrale di sicurezza AWS	Nessun servizio fatturabile utilizzato	0 USD

Servizio	Presupposti	Spese mensili [USD]
Amazon Logs CloudWatch	0,50 USD per GB	< 0,01 USD
AWS Lambda - Richieste	30.000 correzioni * 7 richieste = 210.000 richieste 5.000.000 di risultati * 1 richiesta = 5.000.000 di richieste 0,20 USD/1.000.000 di richieste = 0,0000002 USD per richiesta	1,042 USD
AWS Lambda - Durata	(512 MB di memoria) 4.000 ms * 30.000 riparazioni * 0,0000000083 USD = 0,996 USD 449 ms * 5.000.000 di risultati * 0,0000000083 USD = 18,63 USD	19,63$
AWS Step Functions	19 transizioni di stato * 30.000 riparazioni = 570.000 0,025 USD * (570.000) transizioni di stato = 14,25 USD 000/1	14,25 USD
Regole di Amazon EventBridge	Nessun costo per le regole	0 USD

Servizio	Presupposti	Spese mensili [USD]
AWS Key Management Service	(1 chiave) $1 * 1.000 account * 10 regioni = 10.000$ (richieste Encrypt/Decrypt API) (30.000 correzioni * 2 richieste) + (5.000.000 di risultati * 4 richieste) = 20.060.000 richieste Con la memorizzazione nella cache di AWS KMS: 20.060.000 * 0,30 = 6.018.000 richieste 0,03 USD per 10.000 richieste ⇒ 0,03 USD * (6.018.00 0/10.000) = 18,05 USD	10.018,05 USD
Amazon DynamoDB	2,00$ * (10.000.000 in lettura e scrittura/1.000.000) = 20,00$ (Tabella dei risultati) 15 MB * 1000 account * 10 regioni = 150 GB (Tabella della cronologia) 10 MB * 1000 account * 10 regioni = 100 GB 0,25 USD per GB-month * 250 GB = 62,50 USD	82,50 USD
Amazon SQS	0,40 USD * (5.060.000 richieste/1.000.000) = 2.024 USD	2,024 USD

Servizio	Presupposti	Spese mensili [USD]
Amazon SNS	0,000005 USD * 1.000.000 di notifiche = 0,50 USD	0,50 USD
Amazon CloudWatch - Metriche	(Metriche avanzate disattivate) 0,30 USD * 7 metriche personalizzate = 2,10 USD 0,01 USD * (30.000/1.000) chiamate API put metrics = 0,30 USD	2,40 USD
Amazon CloudWatch - Dashboard	$3,00 * 1 pannello di controllo = $3,00	3,00 USD
Amazon CloudWatch - Allarmi	(Metriche avanzate disattivate) 0,10 USD * 4 allarmi = 0,40 USD	0,40 USD
Amazon CloudWatch - Tracce X-Ray	30.000 correzioni * 7 richieste = 210.000 chiamate Lambda 5.000.000 di risultati * 1 richiesta = 5.000.000 di richiami Lambda 0,000005 USD per traccia * 5.210.000 tracce = 26,05 USD	26,05$
Amazon Cognito	(Livello Essentials) 5.000 utenti attivi mensili	0 USD

Servizio	Presupposti	Spese mensili [USD]
Amazon CloudFront	Trasferimento dati regionale dall'origine (per GB) = 0,020 USD Trasferimento dati regionale verso Internet (per GB) = 0,085 USD Richiedi il prezzo per tutti i metodi HTTP (per 10.000) = 0,0075 USD	0,1125 USD
Simple Storage Service (Amazon S3)	(Hosting dell'interfaccia utente) 0,023 USD per GB * 0,002 GB = 0,000046 USD (Esportazione della cronologia) 0,023 USD per GB * 100 GB = 2,30 USD 0,0004 USD per 1.000 richieste GET * 5.000 richieste = 2,00 USD	4,30 USD

Servizio	Presupposti	Spese mensili [USD]
AWS WAF	1 Web ACL = 5,00 USD al mese 10 regole * 1,00 USD per regola = 10,00 USD (7 gruppi di regole gestite da AWS + 3 regole basate sulla tariffa) Attenuazione intelligente delle minacce con Bot Control = 10,00 USD al mese (più 1,00 USD per 1 milione di richieste e 0,60 USD per 1 milione di richieste WAF, entrambi irrisori se si considerano i volumi di richieste dell'interfaccia utente Web)	25,00 USD
Gateway Amazon API	3,50 USD per milione di chiamate API REST	3,50 USD
Totale		7.393,10$

Important

Costi di rotazione delle chiavi di AWS KMS AWS Key Management Service (AWS KMS) ruota automaticamente le chiavi gestite dai clienti una volta all'anno quando la rotazione è abilitata. Ogni rotazione comporta un costo di 1,00 USD per chiave all'anno. Ad esempio, con 1000 account in una singola regione, si ottengono $ aggiuntivi 1000/year (1 rotazione × 1000 chiavi × 1,00 USD).

Costo aggiuntivo per funzionalità opzionali

Questa sezione identifica i costi aggiuntivi associati alle funzionalità opzionali di questa soluzione.

Metriche migliorate CloudWatch

Se si seleziona `yes` questo EnableEnhancedCloudWatchMetrics parametro durante l'implementazione dello stack di amministrazione, la soluzione crea due metriche personalizzate e un allarme per ogni ID di controllo. Il costo dipende dal numero di ID di controllo che stai correggendo. Nella tabella seguente, si presume che stiate correggendo tutti i 96 diversi ID di controllo al mese, per determinare il limite massimo dei costi.

Servizio	Presupposti 96 ID di controllo * 2 = 192 metriche personalizzate	Spese mensili [USD]
Amazon CloudWatch - Metriche	0,30 USD * 192 metriche personalizzate = 57,60 USD	57,60 USD
Amazon CloudWatch - Allarmi	0,10 USD * 96 allarmi = 9,60 USD	9,60 USD
Totale		67,20$

CloudTrail Registro delle azioni

In ogni account membro per il quale si abilita la funzionalità Action Log, la soluzione crea un CloudTrail percorso per registrare tutti gli eventi di gestione delle scritture. Una funzione Lambda filtra gli eventi non correlati alla soluzione. Ciò significa che il costo è correlato al numero totale di eventi di gestione nel tuo account, poiché gli eventi non correlati alla soluzione vengono comunque rilevati dal percorso ed elaborati dalla funzione Lambda.

Per la tabella seguente, ipotizziamo 150.000 eventi di gestione al mese nell'account. Il costo effettivo dipende dall'effettiva attività degli eventi di gestione nel tuo account.

Servizio	Presupposti	Spese mensili [USD]
AWS CloudTrail	150.000 * 2$. 00/100000 = 3,00 USD	3,00$
Lambda	150.000 * 0,2 * 0,125 = 3.750 GB-seconds	0,0925 USD

Servizio	Presupposti	Spese mensili [USD]
	3.750 * 0,0000166667 USD = costo del tempo di calcolo di 0,0625 USD 0,15 * 0,20 USD = 0,03 USD di costo della richiesta 0,0625 USD + 0,03 USD = costo totale Lambda 0,0925 USD	
Totale		3,09$ per account membro

Sicurezza

Quando crei sistemi sull'infrastruttura AWS, le responsabilità di sicurezza vengono condivise tra te e AWS. Questo modello condiviso riduce il carico operativo perché AWS opera, gestisce e controlla i componenti, tra cui il sistema operativo host, il livello di virtualizzazione e la sicurezza fisica delle strutture in cui operano i servizi. Per ulteriori informazioni sulla sicurezza di AWS, visita AWS Cloud Security.

Politica di sicurezza di API Gateway

Se si sceglie di abilitare l'interfaccia utente Web della soluzione, viene implementata un'API REST API Gateway insieme allo CloudFormation stack di amministrazione che funge da backend per tutte le operazioni nell'interfaccia utente Web. L'API REST distribuita dalla soluzione utilizza la politica di sicurezza TLS predefinita per API Gateway, che è `TLS-1-2` per le API regionali.

Tuttavia, dopo aver distribuito CloudFormation lo stack di amministrazione, puoi scegliere di personalizzare l'API REST della soluzione aggiungendo una politica di sicurezza TLS più restrittiva. Ad esempio, puoi scegliere di `TLS_1_2 security policy` limitare il traffico utilizzando o. TLSv1.2 TLSv1.3 Puoi trovare l'API REST della soluzione nella console API Gateway sotto il nome AutomatedSecurityResponseApi.

Per scegliere una policy di sicurezza per l'API REST della soluzione, devi prima configurare un nome di dominio personalizzato. Per ulteriori informazioni, consulta Nome di dominio personalizzato per le API REST pubbliche in API Gateway.

Per ulteriori informazioni sull'aggiunta di una politica di sicurezza all'API REST, consulta Scegliere una politica di sicurezza per il dominio personalizzato dell'API REST API in API Gateway nella guida API Gateway.

Ruoli IAM

I ruoli AWS Identity and Access Management (IAM) consentono ai clienti di assegnare policy e autorizzazioni di accesso granulari a servizi e utenti nel cloud AWS. Questa soluzione crea ruoli IAM che concedono alle funzioni automatiche della soluzione l'accesso per eseguire azioni correttive nell'ambito di un insieme ristretto di autorizzazioni specifiche per ciascuna correzione.

La Step Function dell'account amministratore è assegnata al ruolo. SO0111-ASR-Orchestrator-Admin Solo questo ruolo può assumere il ruolo SO0111-Orchestrator-Member in ogni account membro. Il ruolo di membro è autorizzato da ciascun ruolo di correzione per passarlo al servizio AWS Systems Manager per eseguire runbook di riparazione specifici. I nomi dei ruoli di riparazione iniziano con SO0111, seguito da una descrizione corrispondente al nome del runbook di riparazione. Ad esempio, SO0111-RemoveVPCDefaultSecurityGroupRules è il ruolo del runbook di riparazione. ASR-RemoveVPCDefaultSecurityGroupRules

Regioni AWS supportate

> **Important**
>
> L'attivazione delle funzionalità opzionali nella soluzione può ridurre l'elenco delle regioni supportate per la distribuzione. In altre parole, l'elenco seguente si applica solo ai componenti principali della soluzione. Ad esempio, se scegli di abilitare l'interfaccia utente Web, non sarai in grado di distribuire la soluzione nelle GovCloud regioni poiché non CloudFront è supportata in GovCloud (Stati Uniti).

Nome della Regione	Codice regione
Stati Uniti orientali (Ohio)	us-east-2
US East (N. Virginia)	us-east-1
Stati Uniti occidentali (California settentrionale)	us-west-1

Nome della Regione	Codice regione
US West (Oregon)	us-west-2
Africa (Città del Capo)	af-south-1
Asia Pacific (Hong Kong)	ap-east-1
Asia Pacifico (Hyderabad)	ap-south-2
Asia Pacifico (Giacarta)	ap-southeast-3
Asia Pacifico (Melbourne)	ap-southeast-4
Asia Pacifico (Mumbai)	ap-south-1
Asia Pacifico (Osaka-Locale)	ap-northeast-3
Asia Pacifico (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Canada (Central)	ca-central-1
Europa (Francoforte)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2
Europe (Milan)	eu-south-1
Europa (Parigi)	eu-west-3
Europa (Spagna)	eu-south-2
Europa (Stoccolma)	eu-north-1

Nome della Regione	Codice regione
Europa (Zurigo)	eu-central-2
Medio Oriente (Bahrein)	me-south-1
Medio Oriente (Emirati Arabi Uniti)	me-central-1
Sud America (San Paolo)	sa-east-1
AWS GovCloud () US-East	us-gov-east-1
AWS GovCloud (US-West)	us-gov-west-1
Cina (Pechino)	cn-north-1
China (Ningxia)	cn-northwest-1
Israele (Tel Aviv)	il-central-1
Canada occidentale (Calgary)	ca-west-1
Messico (Città del Messico)	mx-central-1
Asia Pacifico (Thailandia)	ap-southeast-7
Asia Pacifico (Malesia)	ap-southeast-5
Asia Pacifico (Taipei)	ap-east-2
Asia Pacifico (Nuova Zelanda)	ap-southeast-6

Note

Tutte le nuove regioni AWS non elencate possono essere supportate tramite distribuzione locale ma non tramite distribuzione con un clic.

Quote

Le quote di servizio, anche denominate limiti, rappresentano il numero massimo di risorse di servizio o operazioni per l'account AWS.

Quote per i servizi AWS in questa soluzione

Assicurati di avere una quota sufficiente per ciascuno dei servizi implementati in questa soluzione. Per ulteriori informazioni, consulta le quote dei servizi AWS.

Utilizza i seguenti collegamenti per accedere alla pagina relativa a quel servizio. Per visualizzare le quote di servizio per tutti i servizi AWS nella documentazione senza cambiare pagina, visualizza invece le informazioni nella pagina degli endpoint e delle quote del servizio nel PDF.

Quote AWS CloudFormation

Il tuo account AWS ha delle CloudFormation quote AWS di cui dovresti essere a conoscenza quando avvii lo stack in questa soluzione. Comprendendo queste quote, puoi evitare errori di limitazione che impedirebbero di distribuire con successo questa soluzione. Per ulteriori informazioni, consulta le CloudFormation quote AWS nella Guida per l'utente di AWS CloudFormation .

Quote Amazon CloudWatch

Le CloudWatch quote Amazon del tuo account AWS sono legate alle CloudWatch Resource Policies, che consentono solo 10 politiche relative alle risorse per regione per account e non possono essere aumentate. Per ulteriori informazioni, consulta Amazon CloudWatch Logs Quotas nella Amazon CloudWatch User Guide. Prima della distribuzione, controlla l'utilizzo attuale per assicurarti di non superare questa soglia durante l'implementazione della soluzione.

AWS Organizations

Le funzioni Lambda della soluzione effettuano chiamate all'API https://docs.aws.amazon.com/organizations/latest/APIReference/Welcome.html AWS Organizations per recuperare l'alias dell'account corrente da includere nei messaggi pubblicati nell'argomento SNS della soluzione. Ciò consente di visualizzare i nomi degli account leggibili dall'uomo nelle notifiche della soluzione per scopi di debug e tracciamento.

AWS Organizations impone dei limiti alla frequenza con cui i clienti possono richiamare i propri endpoint API. Se scopri che la soluzione sta superando i limiti impostati per il tuo account, puoi disabilitare la funzionalità che recupera e visualizza l'alias dell'account.

Per fare ciò, accedi alla funzione Lambda denominata `SO0111-ASR-sendNotifications` situata nella regione e nell'account in cui hai distribuito lo stack di amministrazione. Quindi, individua la variabile di ambiente denominata `DISABLE_ACCOUNT_ALIAS_LOOKUP` e modifica il valore da «False» a «True». Il campo dell'alias dell'account nelle notifiche della soluzione sarà ora «Sconosciuto», ma ciò non influirà sulla funzionalità della soluzione.

Limiti e impostazioni predefinite della soluzione

Oltre alle quote di servizio AWS descritte sopra, la soluzione applica i propri limiti predefiniti impostati nella configurazione AWS CDK. Sono configurabili e si collocano ben al di sotto delle quote di servizio AWS sottostanti. Esistono come piani di sicurezza per contenere carichi imprevisti o cicli incontrollati, non come quote ristrette per utente. Le tabelle seguenti elencano i valori che differiscono dal corrispondente servizio AWS predefinito.

Limite	Soluzione predefinita	Servizio AWS predefinito
Amazon API Gateway stage throttle (a livello di account)	500 costanti requests/second , 1.000 raffiche	10.000 requests/second, 5.000 raffica
Limite di frequenza per utente AWS WAF (finestra di 60 secondi)	1.000 richieste	Nessuna regola predefinita
Limite di velocità AWS WAF per IP (finestra di 60 secondi)	2.000 richieste	Nessuna regola predefinita
Limite di velocità di scrittura sensibile di AWS WAF (finestra di 60 secondi)	300 richieste	Nessuna regola predefinita

> **Note**
>
> I limiti di frequenza per utente si aggregano sul token di accesso del chiamante; le richieste prive di tale limite sono coperte dalla regola per IP. Le richieste che superano una regola basata sulla frequenza AWS WAF vengono bloccate e ricevono una risposta HTTP 429 (Too Many Requests) con un corpo JSON.

La soluzione configura anche le seguenti soglie di allarme per l'osservabilità. CloudWatch Questi allarmi notificano gli operatori; non bloccano le richieste.

Allarme	Threshold
Controlla le modifiche allo stato	5 al minuto
Scritti sensibili	20 al minuto

Si applicano le seguenti impostazioni predefinite di calcolo ed elaborazione:

Limite	Soluzione predefinita	Servizio AWS predefinito
Timeout di esecuzione di Orchestrator (AWS Step Functions)	23 ore	1 anno (massimo)
Memoria della funzione Lambda del dispatcher di notifica	256 MB	128 MB
Notification dispatcher (funzione Lambda): concorrenza riservata	10	Nessuno (non riservato)
Timeout della funzione Lambda del dispatcher di notifica	30 secondi (60 secondi per la consegna del webhook)	3 secondi
Conservazione dei messaggi Amazon SQS	14 giorni	4 giorni
Periodo di riutilizzo delle chiavi di dati AWS KMS	60 minuti	5 minuti

La soluzione stabilisce i seguenti limiti di conservazione dei dati (Amazon DynamoDB TTL e Amazon S3) e di esportazione:

Elemento	Soluzione predefinita
Conservazione dei risultati	8 giorni
Conservazione della cronologia delle riparazioni	365 giorni
Conservazione dei file di esportazione	30 giorni
Pre-signed Validità dell'URL	1 giorno
Tempo massimo di esportazione per richiesta	26.000 millisecondi
Numero massimo di record per esportazione	50.000

Distribuzione di AWS Security Hub

La distribuzione e la configurazione di AWS Security Hub sono un prerequisito per questa soluzione. Per ulteriori informazioni sulla configurazione di AWS Security Hub CSPM, consulta la sezione Configurazione di AWS Security Hub CSPM nella Guida per l'utente di AWS Security Hub. Questa soluzione supporta anche AWS Security Hub (versione non CSPM). Per ulteriori informazioni sulla configurazione di AWS Security Hub, consulta Enabling Security Hub.

Come minimo, devi avere un Security Hub funzionante configurato nel tuo account principale. Puoi distribuire questa soluzione nello stesso account (e nella regione AWS) dell'account principale di Security Hub. In ogni account primario e secondario di Security Hub, devi inoltre distribuire il modello di membro che AssumeRole consente alle AWS Step Functions della soluzione di eseguire i runbook di riparazione nell'account.

Stack e distribuzione StackSets

Uno stack set consente di creare stack negli account AWS nelle diverse regioni AWS utilizzando un singolo modello AWS. CloudFormation A partire dalla versione 1.4, questa soluzione supporta la distribuzione di stack set suddividendo le risorse in base a dove e come vengono distribuite. Multi-account i clienti, in particolare quelli che utilizzano AWS Organizations, possono trarre vantaggio dall'utilizzo di stack set per la distribuzione su molti account. Riduce lo sforzo necessario per installare e mantenere la soluzione. Per ulteriori informazioni StackSets, consulta la sezione Utilizzo di AWS CloudFormation StackSets.

Implementazione della soluzione

> **Important**
>
> Se la funzionalità dei risultati di controllo consolidati è attivata in AWS Security Hub, abilita il playbook Security Control (SC) solo durante la distribuzione di questa soluzione. Se la funzionalità non è attivata, abilita solo i playbook per gli standard di sicurezza abilitati in Security Hub. I risultati di controllo consolidati sono abilitati per impostazione predefinita se si abilita Security Hub CSPM a partire dal 23 febbraio 2023.

Questa soluzione utilizza CloudFormation modelli e stack AWS per automatizzarne la distribuzione. I CloudFormation modelli specificano le risorse AWS incluse in questa soluzione e le relative proprietà. Lo CloudFormation stack fornisce le risorse descritte nei modelli.

Affinché la soluzione funzioni, è necessario distribuire tre modelli. Innanzitutto, decidi dove distribuire i modelli, quindi decidi come distribuirli.

Questa panoramica descriverà i modelli e come decidere dove e come distribuirli. Le sezioni successive conterranno istruzioni più dettagliate per la distribuzione di ogni stack come Stack o. StackSet

Decidere dove distribuire ogni stack

I tre modelli saranno denominati con i seguenti nomi e conterranno le seguenti risorse:

- Stack di amministrazione: funzione delle fasi di orchestrator, regole degli eventi e azione personalizzata di Security Hub.
- Stack di membri: documenti di correzione SSM Automation.
- Stack di ruoli dei membri: ruoli IAM per le correzioni.

Lo stack di amministrazione deve essere implementato una volta, in un singolo account e in una singola regione. Deve essere distribuito nell'account e nella regione che hai configurato come destinazione di aggregazione per i risultati di Security Hub per la tua organizzazione. Se desideri utilizzare la funzionalità Action Log per monitorare gli eventi di gestione, devi distribuire lo stack di amministrazione nell'account di gestione dell'organizzazione o in un account amministratore delegato.

La soluzione funziona sui risultati di Security Hub, quindi non sarà in grado di operare sui risultati di un determinato account e regione se tale account o regione non è stato configurato per aggregare i risultati nell'account amministratore e nella regione di Security Hub.

> **Important**
>
> Se utilizzi AWS Security Hub (non CSPM), hai la responsabilità di garantire che gli account dei membri connessi con AWS Security Hub CSPM siano integrati anche con AWS Security Hub (non CSPM). Le regioni aggregate in AWS Security Hub CSPM devono corrispondere anche alle regioni aggregate in AWS Security Hub (non CSPM).

Ad esempio, un'organizzazione dispone di account che operano nelle regioni `us-east-1` e `us-west-2`, con un account `111111111111` come amministratore delegato del Security Hub, nella regione. `us-east-1` Account `222222222222` e `333333333333` devono essere account membri del Security Hub per l'account amministratore delegato. `111111111111` Tutti e tre gli account devono essere configurati per aggregare i risultati da a `us-west-2`. `us-east-1` Lo stack di amministrazione deve essere distribuito sull'account `111111111111` in. `us-east-1`

Per maggiori dettagli sulla ricerca dell'aggregazione, consulta la documentazione per gli account di amministratore delegato di Security Hub e l'aggregazione tra regioni.

Lo stack di amministrazione deve completare la distribuzione prima di distribuire gli stack dei membri in modo da poter creare una relazione di fiducia dagli account dei membri all'account hub.

Lo stack di membri deve essere distribuito in ogni account e regione in cui desideri correggere i problemi. Questo può includere l'account amministratore delegato di Security Hub in cui in precedenza hai distribuito lo stack di amministrazione ASR. I documenti di automazione devono essere eseguiti negli account dei membri per poter utilizzare il livello gratuito per SSM Automation.

Utilizzando l'esempio precedente, se si desidera correggere i risultati di tutti gli account e le regioni, lo stack di membri deve essere distribuito su tutti e tre gli account (`111111111111`, `222222222222`, e `333333333333`) e su entrambe le regioni (e). `us-east-1` `us-west-2`

Lo stack dei ruoli dei membri deve essere distribuito su ogni account, ma contiene risorse globali (ruoli IAM) che possono essere distribuite una sola volta per ogni account. Non importa in quale regione distribuisci lo stack dei ruoli dei membri, quindi, per semplicità, distribuisci lo stack di ruoli dei membri nella stessa regione in cui è distribuito lo stack di amministrazione.

Utilizzando l'esempio precedente, distribuisci lo stack dei ruoli dei membri a tutti e tre gli account (111111111111,222222222222, e) in. 333333333333 us-east-1

Decidere come distribuire ogni stack

Le opzioni per la distribuzione di uno stack sono

- CloudFormation StackSet (autorizzazioni autogestite)
- CloudFormation StackSet (autorizzazioni gestite dal servizio)
- CloudFormation pila

StackSets con autorizzazioni gestite dai servizi sono le più convenienti perché non richiedono l'implementazione di ruoli propri e possono essere distribuite automaticamente a nuovi account dell'organizzazione. Sfortunatamente, questo metodo non supporta gli stack annidati, utilizzati sia nello stack di amministrazione che nello stack dei membri. L'unico stack che può essere distribuito in questo modo è lo stack dei ruoli dei membri.

Tieni presente che quando si esegue la distribuzione nell'intera organizzazione, l'account di gestione dell'organizzazione non è incluso, quindi se si desidera correggere i risultati nell'account di gestione dell'organizzazione, è necessario eseguire la distribuzione in questo account separatamente.

Lo stack di membri deve essere distribuito in ogni account e regione, ma non può essere distribuito utilizzando autorizzazioni gestite dal servizio perché StackSets contiene stack annidati. Distribuisci questo stack con autorizzazioni autogestite. StackSets

Lo stack di amministrazione viene distribuito una sola volta, quindi può essere distribuito come CloudFormation stack semplice o StackSet con autorizzazioni autogestite in un singolo account e regione.

Risultati di controllo consolidati

Gli account dell'organizzazione possono essere configurati con la funzionalità dei risultati di controllo consolidati di Security Hub attivata o disattivata. Consulta i risultati del controllo consolidato nella Guida per l'utente di AWS Security Hub.

> **Important**
>
> Quando questa funzionalità è abilitata, è necessario utilizzare la versione 2.0.0 o successiva della soluzione e abilitare il playbook «SC» (Security Control) sia nello stack Admin che

in quello Member. Questi stack distribuiscono i documenti di automazione necessari per lavorare con ID di controllo consolidati. Non è necessario distribuire stack per singoli standard (come AWS FSBP) quando si utilizzano risultati di controllo consolidati.

Implementazione in Cina

La soluzione supporta l'implementazione nelle regioni cinesi, tuttavia è necessario utilizzare i seguenti pulsanti di avvio per la distribuzione con un clic nelle regioni cinesi, anziché i pulsanti di avvio forniti in altre sezioni di questa guida. L'uso dei pulsanti «Launch Solution» forniti nelle prossime sezioni di questa guida non funzionerà se stai implementando nelle regioni della Cina. Puoi comunque scaricare i modelli da qualsiasi link del bucket S3 e distribuire gli stack caricando il file modello.

- automated-security-response-admin.template:

Launch solution

- automated-security-response-member-roles.template:

Launch solution

- membro.template automated-security-response-response-:

Launch solution

GovCloud distribuzione (USA)

La soluzione supporta l'implementazione nelle regioni GovCloud (Stati Uniti), tuttavia è necessario utilizzare i seguenti pulsanti di avvio per la distribuzione con un clic nelle regioni GovCloud (Stati Uniti), anziché i pulsanti di avvio forniti in altre sezioni di questa guida. L'utilizzo dei pulsanti «Launch Solution» forniti nelle prossime sezioni di questa guida non funzionerà se si esegue la distribuzione

in regioni GovCloud (Stati Uniti). Puoi comunque scaricare i modelli da qualsiasi link del bucket S3 e distribuire gli stack caricando il file modello.

- automated-security-response-admin.template:

- automated-security-response-member-roles.template:

- membro.template automated-security-response-response-:

modelli AWS CloudFormation

automa

security-response-admin.template: utilizza questo modello per avviare la soluzione Automated Security Response on AWS. Il modello installa i componenti principali della soluzione, uno stack annidato per i log di AWS Step Functions e uno stack annidato per ogni standard di sicurezza che scegli di attivare.

I servizi utilizzati includono Amazon Simple Notification Service, AWS Key Management Service, AWS Identity and Access Management, AWS Lambda, AWS Step Functions, Amazon CloudWatch Logs, Amazon S3 e AWS Systems Manager.

Supporto per account amministrativi

I seguenti modelli sono installati nell'account amministratore di AWS Security Hub per attivare gli standard di sicurezza che desideri supportare. Puoi scegliere quale dei seguenti modelli installare durante l'installazione di`automated-security-response-admin.template`.

automated-security-response-orchestrator-log.template - Crea un gruppo di log per la Orchestrator Step Function. CloudWatch

automated-security-response-webui-nested-stack.template - Crea le risorse per supportare l'interfaccia utente Web della soluzione.

AFSBPStack.template- Regole AWS Foundational Security Best Practices v1.0.0.

CIS120Stack.template- Benchmark CIS Amazon Web Services Foundations, regole v1.2.0.

CIS140Stack.template- Benchmark CIS Amazon Web Services Foundations, regole v1.4.0.

CIS300Stack.template- Benchmark CIS Amazon Web Services Foundations, regole v3.0.0.

PCI321Stack.template- PCI-DSS regole v3.2.1.

NISTStack.template- Regole del National Institute of Standards and Technology (NIST), v5.0.0.

SCStack.template- Regole di Security Controls v2.0.0.

Ruoli dei membri

View template automa

security-response-member-roles.template: definisce i ruoli di correzione necessari in ogni account membro di AWS Security Hub.

Account membri

View template automa

security-response-member.template: utilizza questo modello dopo aver configurato la soluzione di base per installare i runbook e le autorizzazioni di automazione di AWS Systems Manager in ciascuno dei tuoi account membri di AWS Security Hub (incluso l'account amministratore). Questo modello consente di scegliere quali playbook standard di sicurezza installare.

`automated-security-response-member.template`Installa i seguenti modelli in base alle tue selezioni:

automated-security-response-remediation-runbooks.template - Codice di riparazione comune utilizzato da uno o più standard di sicurezza.

AFSBPMemberStack.template- Impostazioni, autorizzazioni e runbook di riparazione di AWS Foundational Security Best Practices v1.0.0.

CIS120MemberStack.template- Benchmark CIS Amazon Web Services Foundations, impostazioni, autorizzazioni e runbook di riparazione della versione 1.2.0.

CIS140MemberStack.template- Benchmark CIS Amazon Web Services Foundations, impostazioni, autorizzazioni e runbook di riparazione della versione 1.4.0.

CIS300MemberStack.template- Benchmark CIS Amazon Web Services Foundations, impostazioni, autorizzazioni e runbook di riparazione della versione 3.0.0.

PCI321MemberStack.template- impostazioni, autorizzazioni e runbook di PCI-DSS riparazione v3.2.1.

NISTMemberStack.template- National Institute of Standards and Technology (NIST), v5.0.0, impostazioni, autorizzazioni e runbook di riparazione.

SCMemberStack.template- Impostazioni, autorizzazioni e runbook di riparazione di Security Control.

automated-security-response-member-cloudtrail.template - Utilizzato nella funzione Action Log per tracciare e controllare l'attività del servizio.

Integrazione del sistema di ticket

Utilizza uno dei seguenti modelli per l'integrazione con il tuo sistema di biglietteria.

JiraBlu

Implementa se usi Jira come sistema di biglietteria.

Service

Implementa se lo usi ServiceNow come sistema di biglietteria.

Se desideri integrare un diverso sistema di ticketing esterno, puoi utilizzare uno di questi stack come modello per capire come implementare la tua integrazione personalizzata.

Implementazione automatizzata - StackSets

> **Note**
>
> Ti consigliamo di eseguire la distribuzione con. StackSets Tuttavia, per le distribuzioni con un singolo account o per scopi di test o valutazione, considera l'opzione di distribuzione degli stack.

Prima di lanciare la soluzione, esaminate l'architettura, i componenti della soluzione, la sicurezza e le considerazioni di progettazione discusse in questa guida. Segui le istruzioni dettagliate in questa sezione per configurare e distribuire la soluzione nelle tue organizzazioni AWS.

Tempo di distribuzione: circa 30 minuti per account, a seconda dei parametri. StackSet

Prerequisiti

AWS Organizations ti aiuta a gestire e governare centralmente l'ambiente e le risorse AWS con più account. StackSets funziona al meglio con AWS Organizations.

Se hai già installato la versione 1.3.x o una versione precedente di questa soluzione, devi disinstallare la soluzione esistente. Per ulteriori informazioni, fare riferimento a Aggiornare la soluzione. ???

Prima di distribuire questa soluzione, rivedi la tua distribuzione di AWS Security Hub:

- Nella tua organizzazione AWS deve essere presente un account amministratore delegato di Security Hub.
- Security Hub deve essere configurato per aggregare i risultati tra le regioni. Per ulteriori informazioni, consulta Aggregazione dei risultati tra le regioni nella Guida per l'utente di AWS Security Hub.
- Dovresti attivare Security Hub per la tua organizzazione in ogni regione in cui utilizzi AWS.

Questa procedura presuppone che tu disponga di più account che utilizzano AWS Organizations e che tu abbia delegato un account amministratore di AWS Organizations e un account amministratore di AWS Security Hub.

Questa soluzione funziona sia con AWS Security Hub che con AWS Security Hub CSPM.

Panoramica dell'implementazione

> **Note**
>
> StackSets l'implementazione di questa soluzione utilizza una combinazione di servizi gestiti e autogestiti. StackSets Self-managed StackSets devono essere utilizzati attualmente perché utilizzano stack annidati, che non sono ancora supportati da service-managed. StackSets

Distribuiscili StackSets da un account amministratore delegato nelle tue organizzazioni AWS.

Pianificazione

Usa il seguente modulo per facilitare la distribuzione. StackSets Prepara i dati, quindi copia e incolla i valori durante la distribuzione.

```
AWS Organizations admin account ID: _________________
Security Hub admin account ID: _________________
CloudTrail Logs Group: ____________________________
Member account IDs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
AWS Organizations OUs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
```

(Facoltativo) Passaggio 0: implementa lo stack di integrazione dei ticket

- Se intendi utilizzare la funzione di ticketing, implementa prima lo stack di integrazione dei ticket nel tuo account amministratore di Security Hub.
- Copia il nome della funzione Lambda da questo stack e forniscilo come input allo stack di amministrazione (vedi Passaggio 1).

Passaggio 1: avvia lo stack di amministrazione nell'account amministratore delegato di Security Hub

- Utilizzando un modello autogestito StackSet, avvia il CloudFormation modello `automated-security-response-admin.template` AWS nel tuo account amministratore di AWS Security Hub nella stessa regione dell'amministratore di Security Hub. Questo modello utilizza stack annidati.
- Scegli quali standard di sicurezza installare. Per impostazione predefinita, è selezionato solo SC (consigliato).
- Scegliete un gruppo di log di Orchestrator esistente da utilizzare. Scegli `Yes` se esiste `SO0111-ASR-Orchestrator` già da un'installazione precedente.
- Scegli se abilitare l'interfaccia utente Web della soluzione. Se scegli di abilitare questa funzionalità, devi anche inserire un indirizzo email a cui assegnare un ruolo di amministratore.
- Scegli le tue preferenze per la raccolta CloudWatch delle metriche relative allo stato operativo della soluzione.

Per ulteriori informazioni sull'autogestione StackSets, consulta la sezione Concessione di autorizzazioni autogestite nella AWS User Guide. CloudFormation

Passaggio 2: installa i ruoli di correzione in ogni account membro di AWS Security Hub

Attendi il completamento della distribuzione nella Fase 1, perché il modello nella Fase 2 fa riferimento ai ruoli IAM creati dalla Fase 1.

- Utilizzando un servizio gestito StackSet, avvia il CloudFormation modello `automated-security-response-member-roles.template` AWS in una singola regione in ogni account delle tue organizzazioni AWS.
- Scegli di installare questo modello automaticamente quando un nuovo account entra a far parte dell'organizzazione.
- Inserisci l'ID dell'account amministratore di AWS Security Hub.
- Inserisci un valore `namespace` che verrà utilizzato per evitare conflitti tra i nomi delle risorse e una distribuzione precedente o contemporanea nello stesso account. Inserisci una stringa composta da un massimo di 9 caratteri alfanumerici minuscoli.

Passaggio 3: avvia lo stack di membri in ogni account e regione membro di AWS Security Hub

- In modalità autogestita StackSets, avvia il CloudFormation modello `automated-security-response-member.template` AWS in tutte le regioni in cui sono presenti risorse AWS in ogni account della tua organizzazione AWS gestito dallo stesso amministratore di Security Hub.

> **Note**
>
> Fino agli stack annidati del StackSets supporto gestito dal servizio, devi eseguire questo passaggio per tutti i nuovi account che entrano a far parte dell'organizzazione.

- Scegli quali playbook Security Standard installare.
- Fornisci il nome di un gruppo di CloudTrail log (utilizzato per alcune correzioni).
- Inserisci l'ID dell'account amministratore di AWS Security Hub.
- Inserisci un valore `namespace` che verrà utilizzato per evitare conflitti tra i nomi delle risorse e una distribuzione precedente o contemporanea nello stesso account. Inserisci una stringa composta da un massimo di 9 caratteri alfanumerici minuscoli. Dovrebbe corrispondere al `namespace` valore selezionato per lo stack dei ruoli dei membri. Inoltre, il valore dello spazio dei nomi non deve essere univoco per account membro.

(Facoltativo) Passaggio 0: Avvia uno stack di integrazione del sistema di ticket

1. Se intendi utilizzare la funzione di ticketing, avvia prima il rispettivo stack di integrazione.
2. Scegli gli stack di integrazione forniti per Jira o ServiceNow, oppure usali come modello per implementare la tua integrazione personalizzata.

   Per distribuire lo stack Jira:

   a. Inserisci un nome per il tuo stack.

   b. Fornisci l'URI alla tua istanza Jira.

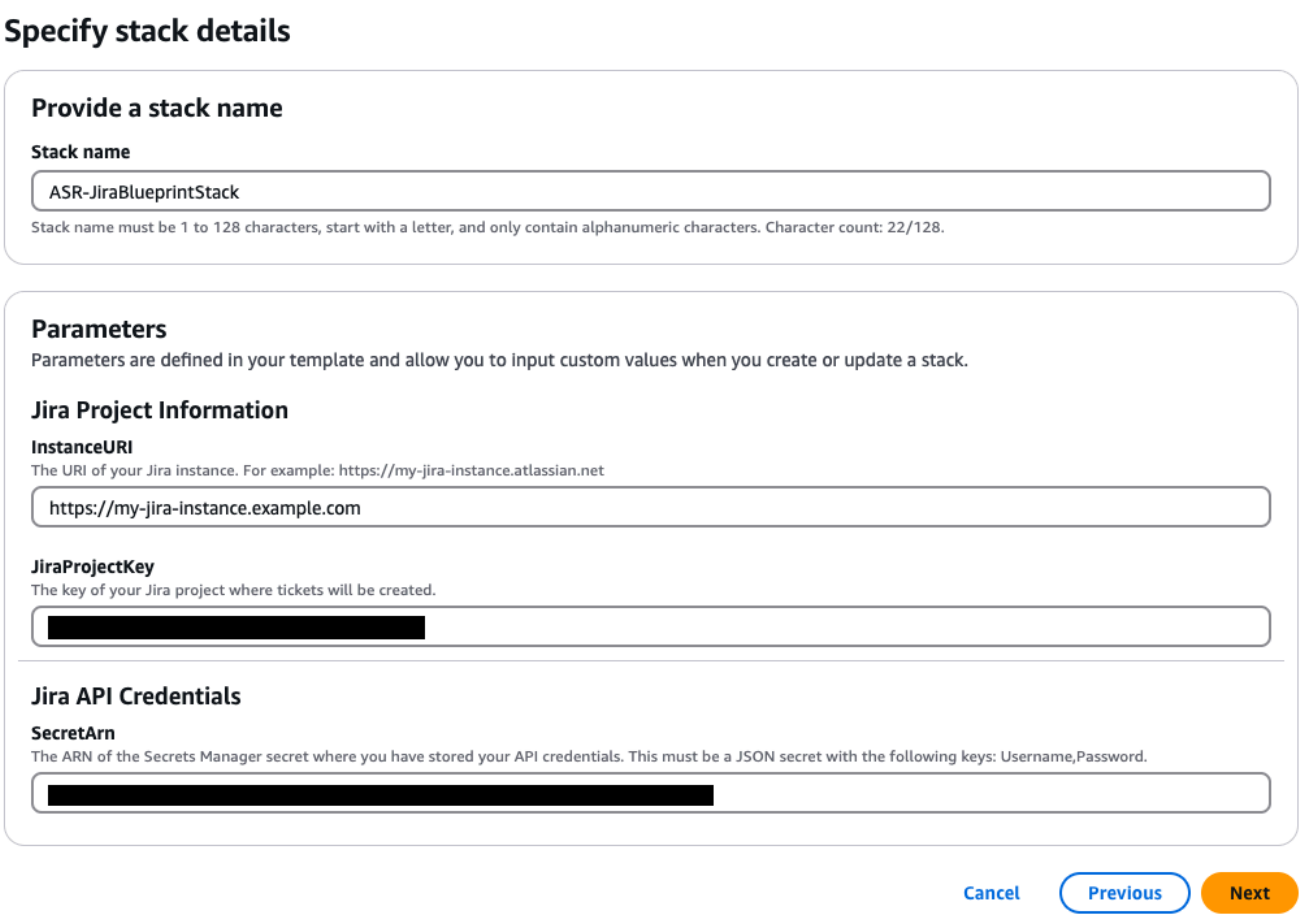
   c. Fornisci la chiave di progetto per il progetto Jira a cui desideri inviare i ticket.

   d. Crea un nuovo segreto chiave-valore in AWS Secrets Manager che contiene Jira e. `Username` `Password`

   > **Note**
   >
   > Puoi scegliere di utilizzare una chiave API Jira al posto della tua password fornendo il tuo nome utente come `Username` e la tua chiave API come. `Password`

   e. Aggiungi l'ARN di questo segreto come input allo stack.

Fornisci il nome dello stack, le informazioni sul progetto Jira e le credenziali dell'API Jira.



Configurazione di Jira Field:

Dopo aver distribuito lo stack Jira, puoi personalizzare i campi del ticket di Jira impostando la variabile di `JIRA_FIELDS_MAPPING` ambiente sulla funzione Lambda. Questa stringa JSON sovrascrive i campi predefiniti del ticket Jira e deve seguire la struttura dei campi dell'API Jira.

Valori predefiniti quando `JIRA_FIELDS_MAPPING` è vuoto o i campi non sono specificati:

- priorità: `{"id": "3"}` (priorità media)
- tipo di problema: `{"id": "10006"}` (Attività)
- AccountID: recuperato automaticamente utilizzando l'endpoint API `GET /rest/api/2/myself`

  Esempio di configurazione con campi personalizzati:

```
{
  "reporter": {"accountId": "123456:494dcbff-1b80-482c-a89d-56ae81c145a4"},
  "priority": {"id": "1"},
  "issuetype": {"id": "10006"},
  "assignee": {"accountId": "123456:another-user-id"},
  "customfield_10001": "custom value"
}
```

ID di campo Jira comuni:

- ID di priorità: 1 (massimo), 2 (alto), 3 (medio), 4 (basso), 5 (minimo)
- ID del tipo di problema: varia in base al progetto Jira (ad esempio, 10006 per Task)
- ID account: formato `123456:494dcbff-1b80-482c-a89d-56ae81c145a4`

Puoi trovare gli ID di campo e gli ID account di Jira utilizzando l'API REST di Jira:

- `GET /rest/api/2/myself`per l'ID dell'account
- `GET /rest/api/2/priority`per gli ID prioritari
- `GET /rest/api/2/project/{projectKey}`per gli ID dei tipi di problema

Per ulteriori informazioni, consulta il formato Jira REST API v2 Issue POST.

Per distribuire lo stack: ServiceNow

f. Inserisci un nome per il tuo stack.

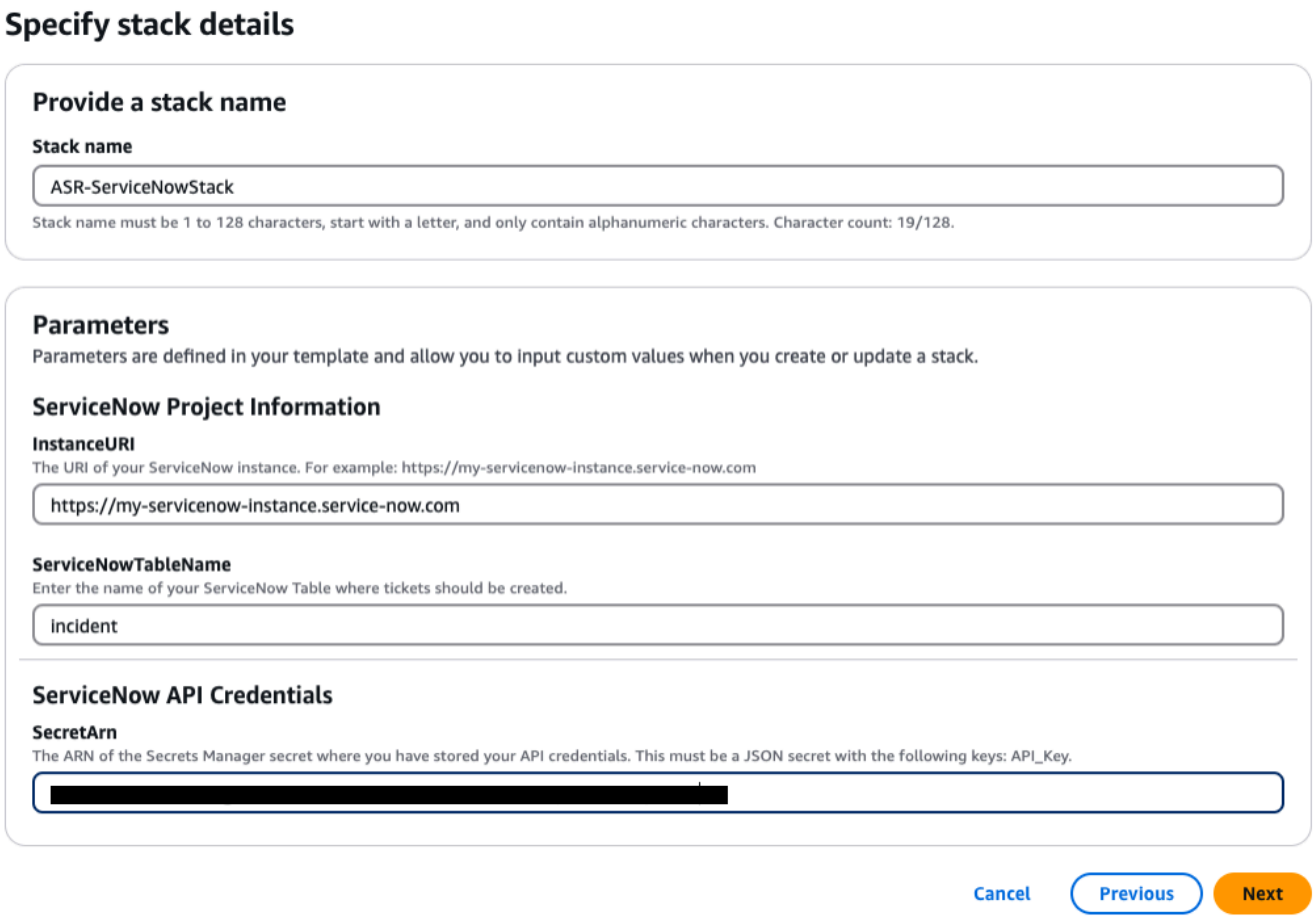
g. Fornisci l'URI della tua ServiceNow istanza.

h. Fornisci il nome della tua ServiceNow tabella.

i. Crea una chiave API ServiceNow con il permesso di modificare la tabella su cui intendi scrivere.

j. Crea un segreto in Secrets Manager con la chiave `API_Key` e fornisci l'ARN segreto come input per lo stack.

Fornisci il nome dello stack, le informazioni sul ServiceNow progetto e le credenziali ServiceNow API.



Per creare uno stack di integrazione personalizzato: includi una funzione Lambda che l'orchestrator della soluzione Step Functions può chiamare per ogni correzione. La funzione Lambda dovrebbe prendere l'input fornito da Step Functions, creare un payload in base ai requisiti del sistema di ticketing e inviare una richiesta al sistema per creare il ticket.

Passaggio 1: avvia lo stack di amministrazione nell'account amministratore delegato di Security Hub

1. Avvia lo stack di amministrazione con `automated-security-response-admin.template` il tuo account amministratore di Security Hub. In genere, uno per organizzazione in una singola regione. Poiché questo stack utilizza stack annidati, è necessario distribuire questo modello in modalità autogestita. StackSet

Parameters

Parametro	Predefinita	Description
Carica SC Admin Stack	`yes`	Specifica se installare i componenti di amministr azione per la correzione automatica dei controlli SC.
Carica lo stack di amministr azione AFSBP	no	Specifica se installare i componenti di amministr azione per la correzione automatica dei controlli FSBP.
Carica CIS120 Admin Stack	no	Specifica se installare i componenti di amministr azione per la correzion e automatica dei controlli CIS120.
Carica CIS140 Admin Stack	no	Specifica se installare i componenti di amministr azione per la correzion e automatica dei controlli CIS140.
Carica CIS300 Admin Stack	no	Specifica se installare i componenti di amministr azione per la correzion e automatica dei controlli CIS300.
Carica lo stack di amministr azione PCI321	no	Specifica se installare i componenti di amministr azione per la correzion e automatica dei controlli PCI321.

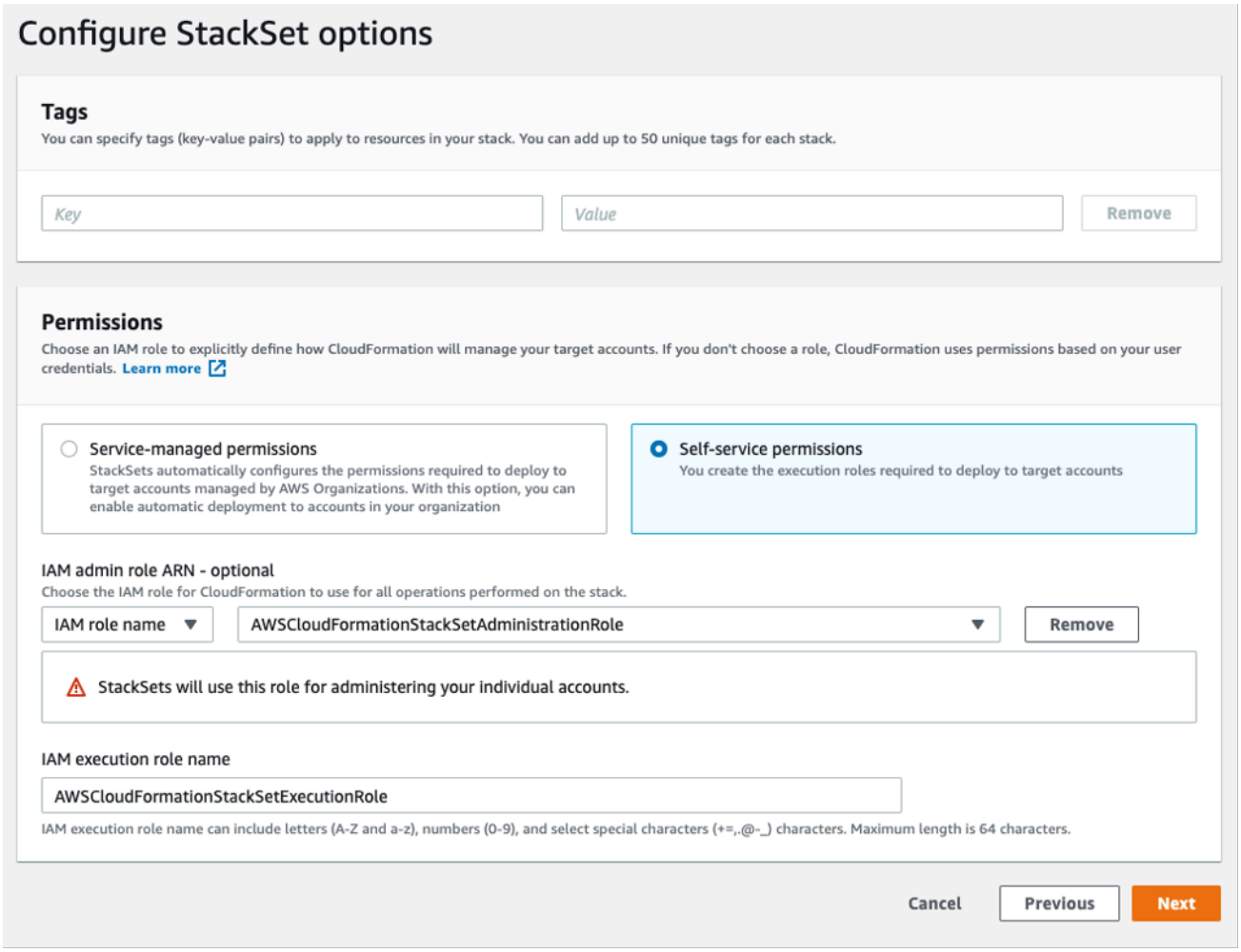
Parametro	Predefinita	Description
Carica NIST Admin Stack	no	Specifica se installare i componenti di amministr azione per la correzione automatica dei controlli NIST.
Riutilizza Orchestrator Log Group	no	Seleziona se riutilizzare o meno un gruppo di log esistente. `SO0111-ASR-Orchestrator` CloudWatch Ciò semplifica la reinstallazione e gli aggiornamenti senza perdere i dati di registro di una versione precedente. Riutilizza quelli esistenti, `Orchestrator Log Group` scegli `yes` se `Orchestrator Log Group` sono ancora presenti in una distribuzione precedente in questo account, altrimenti. no Se stai eseguendo un aggiornamento dello stack da una versione precedente alla v2.3.0, scegli no

Parametro	Predefinita	Description
ShouldDeployWebUI	`yes`	Implementa i componenti dell'interfaccia utente Web tra cui API Gateway, funzioni Lambda e distribuzione. CloudFront Scegli «sì» per abilitare l'interfaccia utente basata sul Web per visualizz are i risultati e lo stato della correzione. Se scegli di disabilitare questa funzional ità, puoi comunque configura re le correzioni automatiche ed eseguirle su richiesta utilizzan do l'azione personalizzata Security Hub CSPM.
AdminUserEmail	(Inserimento opzionale)	Indirizzo email dell'uten te amministratore iniziale. Questo utente avrà accesso amministrativo completo all'interfaccia utente Web ASR. Richiesto solo quando l'interfaccia utente Web è abilitata.
Usa le CloudWatch metriche	`yes`	Specifica se abilitare le CloudWatch metriche per il monitoraggio della soluzione . Verrà creata una CloudWatc h dashboard per la visualizz azione delle metriche.

Parametro	Predefinita	Description
Usa le CloudWatch metriche e gli allarmi	`yes`	Specifica se abilitare gli allarmi CloudWatch metrici per la soluzione. Questo creerà allarmi per determina te metriche raccolte dalla soluzione.
RemediationFailureAlarmThreshold	5	Specifica la soglia per la percentuale di errori di riparazione per ID di controllo . Ad esempio, se si immette5, si riceve un avviso se un ID di controllo non supera più del 5% delle correzioni in un determinato giorno. Questo parametro funziona solo se vengono creati allarmi (vedi il parametro Use CloudWatch Metrics Alarms).
EnableEnhancedCloudWatchMetrics	no	Seyes, crea CloudWatch metriche aggiuntive per tenere traccia di tutti gli ID di controllo singolarmente sulla CloudWatch dashboard e come allarmi. CloudWatch Consulta la sezione Costo per comprendere i costi aggiuntivi che ciò comporta.

Parametro	Predefinita	Description
TicketGenFunctionName	(Inserimento opzionale)	Opzionale. Lascia vuoto se non desideri integrare un sistema di biglietteria. Altrimenti, fornisci il nome della funzione Lambda dall'output dello stack di Step 0, ad esempio:. `SO0111-ASR-ServiceNow-TicketGenerator`

Configura le opzioni StackSet



1. Per il parametro Account numbers, inserisci l'ID dell'account amministratore di AWS Security Hub.
2. Per il parametro Specify regions, seleziona solo la regione in cui è attivato l'amministratore di Security Hub. Attendi il completamento di questo passaggio prima di passare al passaggio 2.

   Puoi visualizzare lo stato dell' StackSet operazione nella CloudFormation console AWS nella pagina dei StackSet dettagli. Dovresti ricevere lo stato dell'operazione RIUSCITO in circa 15 minuti.

Passaggio 2: installa i ruoli di correzione in ogni account membro di AWS Security Hub

Utilizza un servizio gestito StackSets per distribuire il modello dei ruoli dei membri,. `automated-security-response-member-roles.template` Questo StackSet deve essere distribuito in una regione per account membro. Definisce i ruoli globali che consentono le chiamate API tra più account dalla funzione step di ASR Orchestrator.

Parameters

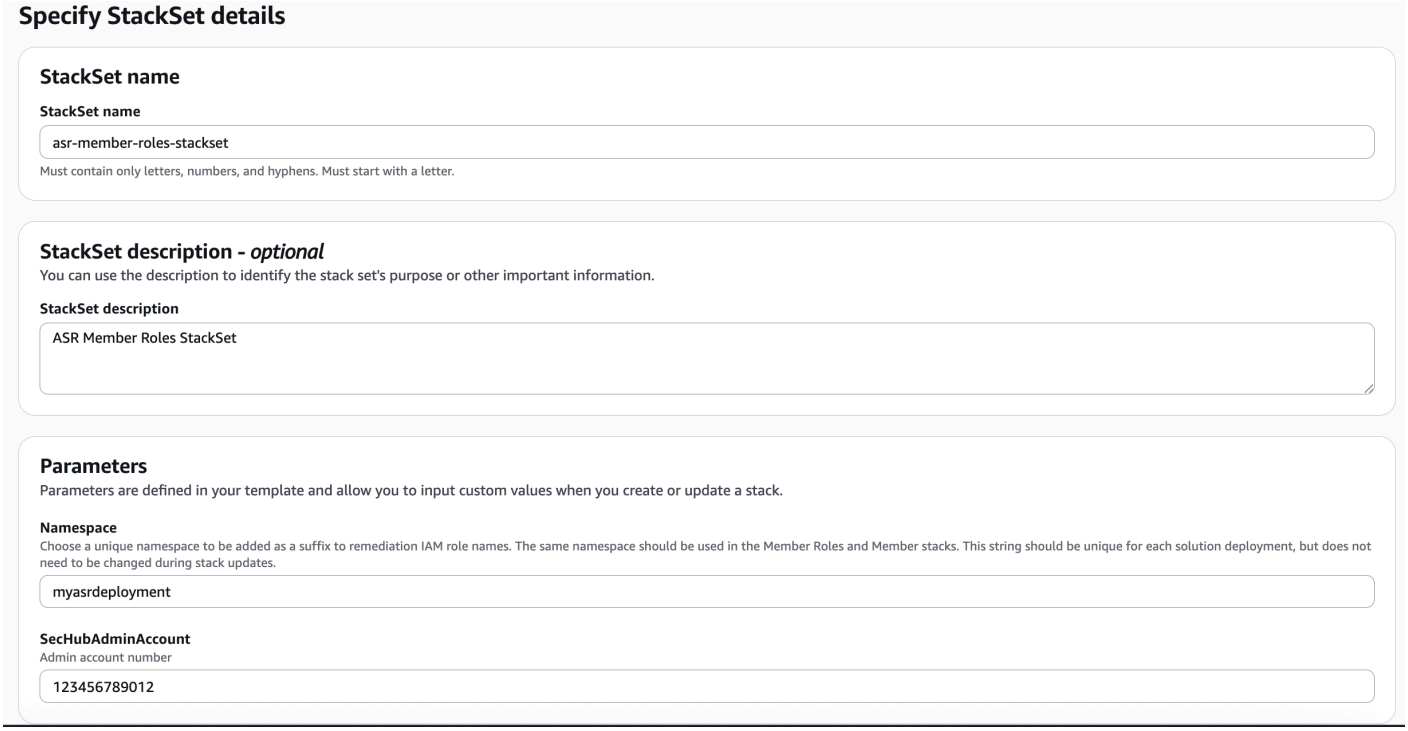
Parametro	Predefinita	Description
Spazio dei nomi	*<Requires input>*	Inserisci una stringa composta da un massimo di 9 caratteri alfanumerici minuscoli. Namespace univoco da aggiungere come suffisso ai nomi dei ruoli IAM di Remediation. Lo stesso namespace deve essere utilizzato nei ruoli dei membri e negli stack dei membri. Questa stringa deve essere univoca per ogni distribuzione della soluzione, ma non deve essere modificata durante gli aggiornamenti dello stack.

Parametro	Predefinita	Description
		Non è necessario che il valore dello spazio dei nomi sia univoco per account membro.
Account amministratore Sec Hub	*<Requires input>*	Inserisci l'ID dell'account di 12 cifre per l'account amministratore di AWS Security Hub. Questo valore concede le autorizzazioni per il ruolo di soluzione dell'account amministratore.

1. Esegui la distribuzione nell'intera organizzazione (tipica) o nelle unità organizzative, in base alle politiche della tua organizzazione.
2. Attiva la distribuzione automatica in modo che i nuovi account in AWS Organizations ricevano queste autorizzazioni.
3. Per il parametro Specify regions, seleziona una singola regione. I ruoli IAM sono globali. Puoi continuare con la Fase 3 mentre questa operazione StackSet viene implementata.

   Puoi visualizzare lo stato dell' StackSet operazione nella CloudFormation console AWS nella pagina dei StackSet dettagli. Dovresti ricevere lo stato dell'operazione RIUSCITO in circa 5 minuti.

   Specifica i dettagli StackSet



Fase 3: Avvia lo stack di membri in ogni account e regione membro di AWS Security Hub

Poiché lo stack di membri utilizza stack annidati, è necessario eseguire l'implementazione in modalità autogestita. StackSet Ciò non supporta la distribuzione automatica su nuovi account nell'organizzazione AWS.

Parameters

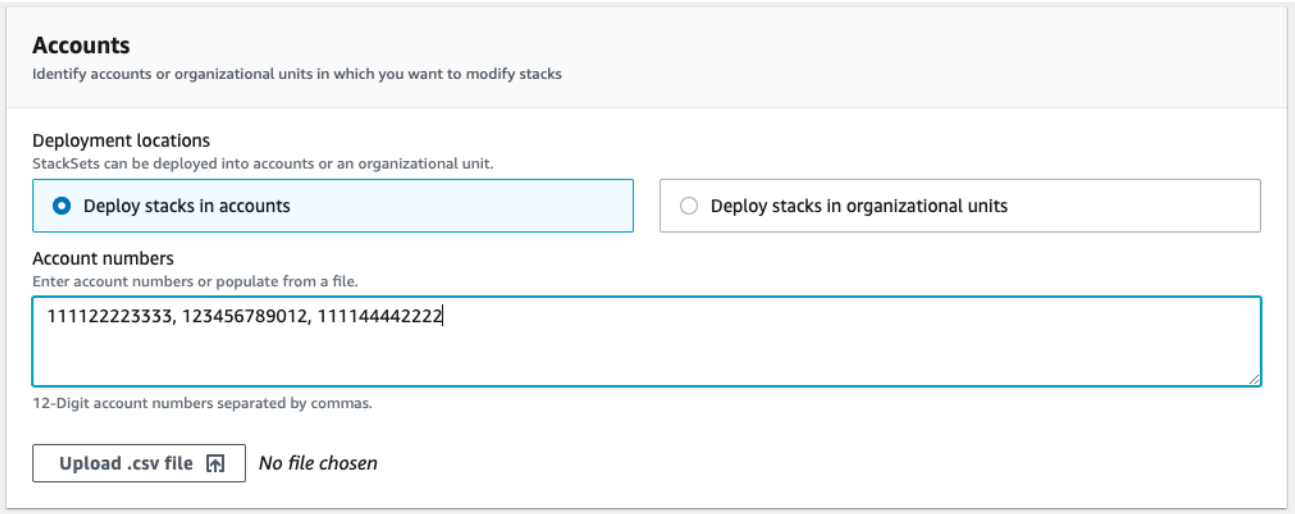
Parametro	Predefinita	Description
Fornisci il nome LogGroup da utilizzare per creare filtri metrici e allarmi	*<Requires input>*	Specifica il nome di un gruppo di CloudWatch CloudTrail log in cui vengono registrate le chiamate API. Viene utilizzato per le correzioni CIS 3.1-3.14.
Carica SC Member Stack	`yes`	Specifica se installare i componenti dei membri per

Parametro	Predefinita	Description
		la correzione automatica dei controlli SC.
Carica AFSBP Member Stack	no	Specifica se installare i componenti dei membri per la correzione automatica dei controlli FSBP.
Carica lo stack di membri CIS120	no	Specificare se installare i componenti membri per la riparazione automatica dei controlli CIS120.
Carica lo stack di membri CIS140	no	Specificare se installare i componenti membri per la riparazione automatica dei controlli CIS140.
Carica lo stack di membri CIS300	no	Specifica se installare i componenti membri per la correzione automatica dei controlli CIS300.
Carica PCI321 Member Stack	no	Specifica se installare i componenti membri per la correzione automatica dei controlli PCI321.
Carica NIST Member Stack	no	Specifica se installare i componenti dei membri per la correzione automatica dei controlli NIST.

Parametro	Predefinita	Description
Crea un bucket S3 per Redshift Audit Logging	no	Scegli `yes` di creare il bucket S3 per la correzione FSBP. RedShift.4 Per i dettagli sul bucket S3 e sulla correzione, consulta la correzione nella Guida per l'utente di AWS Security Redshift.4 Hub.
Account amministratore Sec Hub	*<Requires input>*	Inserisci l'ID dell'account di 12 cifre per l'account amministr atore di AWS Security Hub.
Spazio dei nomi	*<Requires input>*	Inserisci una stringa composta da un massimo di 9 caratteri alfanumerici minuscoli. Questa stringa diventa parte dei nomi dei ruoli IAM e del bucket Action Log S3. Utilizza lo stesso valore per la distribuz ione dello stack dei membri e per la distribuzione dello stack dei ruoli dei membri. La stringa deve essere univoca per ogni distribuzione della soluzione, ma non deve essere modificat a durante gli aggiornamenti dello stack.

Parametro	Predefinita	Description
EnableCloudTrailForASRActionLog	no	Seleziona `yes` se desideri monitorare gli eventi di gestione condotti dalla soluzione sulla CloudWatch dashboard. La soluzione crea un CloudTrail percorso nell'account di ogni membro selezionato`yes`. È necessario distribuire la soluzione in un'organizzazione AWS per abilitare questa funzionalità. Inoltre, puoi abilitare questa funzionalità solo in una singola regione all'interno dello stesso account. Consulta la sezione Costo per comprendere i costi aggiuntivi che ciò comporta.

Account



Sedi di distribuzione: è possibile specificare un elenco di numeri di account o unità organizzative.

Specifica le regioni: seleziona tutte le regioni in cui desideri correggere i risultati. Puoi modificare le opzioni di distribuzione in base al numero di account e alle regioni. La concorrenza tra regioni può essere parallela.

Puoi visualizzare lo stato dell' StackSet operazione nella CloudFormation console AWS nella pagina dei StackSet dettagli. Dovresti ricevere lo stato dell'operazione RIUSCITA per ogni combinazione di account e regione. Il tempo di distribuzione varia in base al numero di account e alle regioni selezionate.

Distribuzione automatizzata: Stacks

> **Note**
>
> Per i clienti con più account, consigliamo vivamente l'implementazione con. StackSets

Prima di lanciare la soluzione, esaminate l'architettura, i componenti della soluzione, la sicurezza e le considerazioni di progettazione discusse in questa guida. Segui le istruzioni dettagliate in questa sezione per configurare e distribuire la soluzione nel tuo account.

Tempo di implementazione: circa 30 minuti

Prerequisiti

Prima di distribuire questa soluzione, assicurati che AWS Security Hub si trovi nella stessa regione AWS dei tuoi account primari e secondari. Se hai già distribuito questa soluzione, devi disinstallare la soluzione esistente. Per ulteriori informazioni, consulta Aggiornare la soluzione.

Panoramica sull'implementazione

Utilizza i seguenti passaggi per distribuire questa soluzione su AWS.

(Facoltativo) Passaggio 0: avvio di uno stack di integrazione del sistema di ticket

- Se intendi utilizzare la funzione di ticketing, implementa prima lo stack di integrazione dei ticket nel tuo account amministratore di Security Hub.
- Copia il nome della funzione Lambda da questo stack e forniscilo come input allo stack di amministrazione (vedi Passaggio 1).

Passaggio 1: avvia lo stack di amministrazione

- Avvia il CloudFormation modello `automated-security-response-admin.template` AWS nel tuo account amministratore di AWS Security Hub.
- Scegli gli standard di sicurezza da installare.
- Scegli un gruppo di log di Orchestrator esistente da utilizzare (scegli `Yes` se esiste `SO0111-ASR-Orchestrator` già da un'installazione precedente).

Passaggio 2: installa i ruoli di correzione in ogni account membro di AWS Security Hub

- Avvia il CloudFormation modello `automated-security-response-member-roles.template` AWS in una regione per account membro.
- Inserisci l'ID dell'account di 12 cifre per l'account amministratore di AWS Security Hub.

Passaggio 3: avvia lo stack di membri

- Specificare il nome del gruppo CloudWatch Logs da utilizzare con le correzioni CIS 3.1-3.14. Deve essere il nome di un gruppo di CloudWatch log Logs che riceve i log. CloudTrail
- Scegli se installare i ruoli di correzione. Installa questi ruoli solo una volta per ogni account.
- Scegli quali playbook installare.
- Inserisci l'ID dell'account amministratore di AWS Security Hub.

Fase 4: (Facoltativo) Modifica le correzioni disponibili

- Rimuovi eventuali rimedi in base all'account per membro. Questa fase è facoltativa.

(Facoltativo) Passaggio 0: Avvia uno stack di integrazione del sistema di ticket

1. Se intendi utilizzare la funzione di ticketing, avvia prima il rispettivo stack di integrazione.
2. Scegli gli stack di integrazione forniti per Jira o ServiceNow, oppure usali come modello per implementare la tua integrazione personalizzata.

   Per distribuire lo stack Jira:

   a. Inserisci un nome per il tuo stack.

b. Fornisci l'URI alla tua istanza Jira.

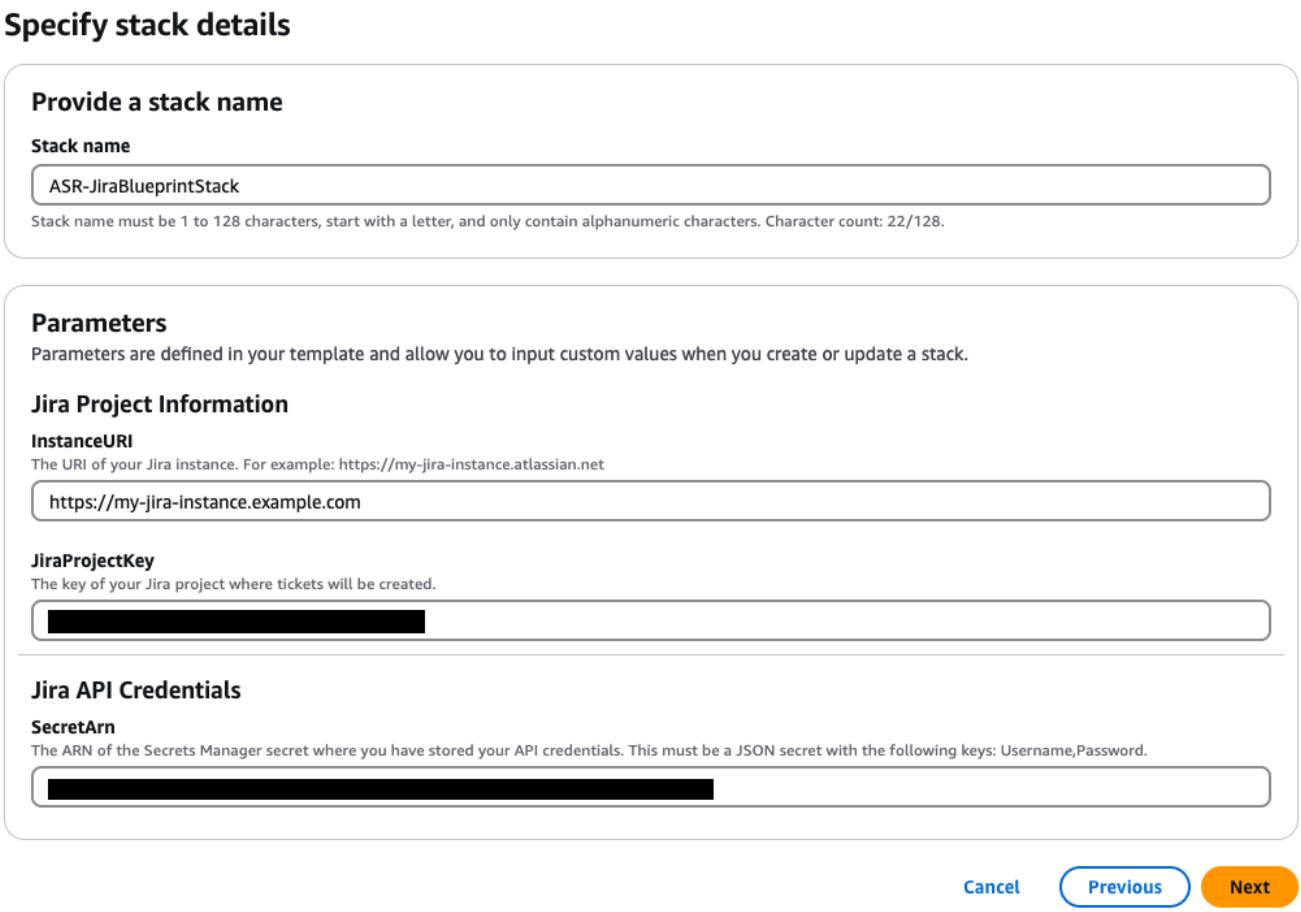
c. Fornisci la chiave di progetto per il progetto Jira a cui desideri inviare i ticket.

d. Crea un nuovo segreto chiave-valore in Secrets Manager che contiene Jira e. `Username` `Password`

> **Note**
>
> Puoi scegliere di utilizzare una chiave API Jira al posto della tua password fornendo il tuo nome utente come `Username` e la tua chiave API come. `Password`

e. Aggiungi l'ARN di questo segreto come input allo stack.

Fornisci il nome dello stack, le informazioni sul progetto Jira e le credenziali dell'API Jira.



Configurazione di Jira Field:

Per informazioni sulla personalizzazione dei campi dei ticket di Jira, consulta la sezione Jira Field Configuration nel Passaggio 0 della distribuzione. StackSet

Per distribuire lo stack: ServiceNow

f. Inserisci un nome per il tuo stack.

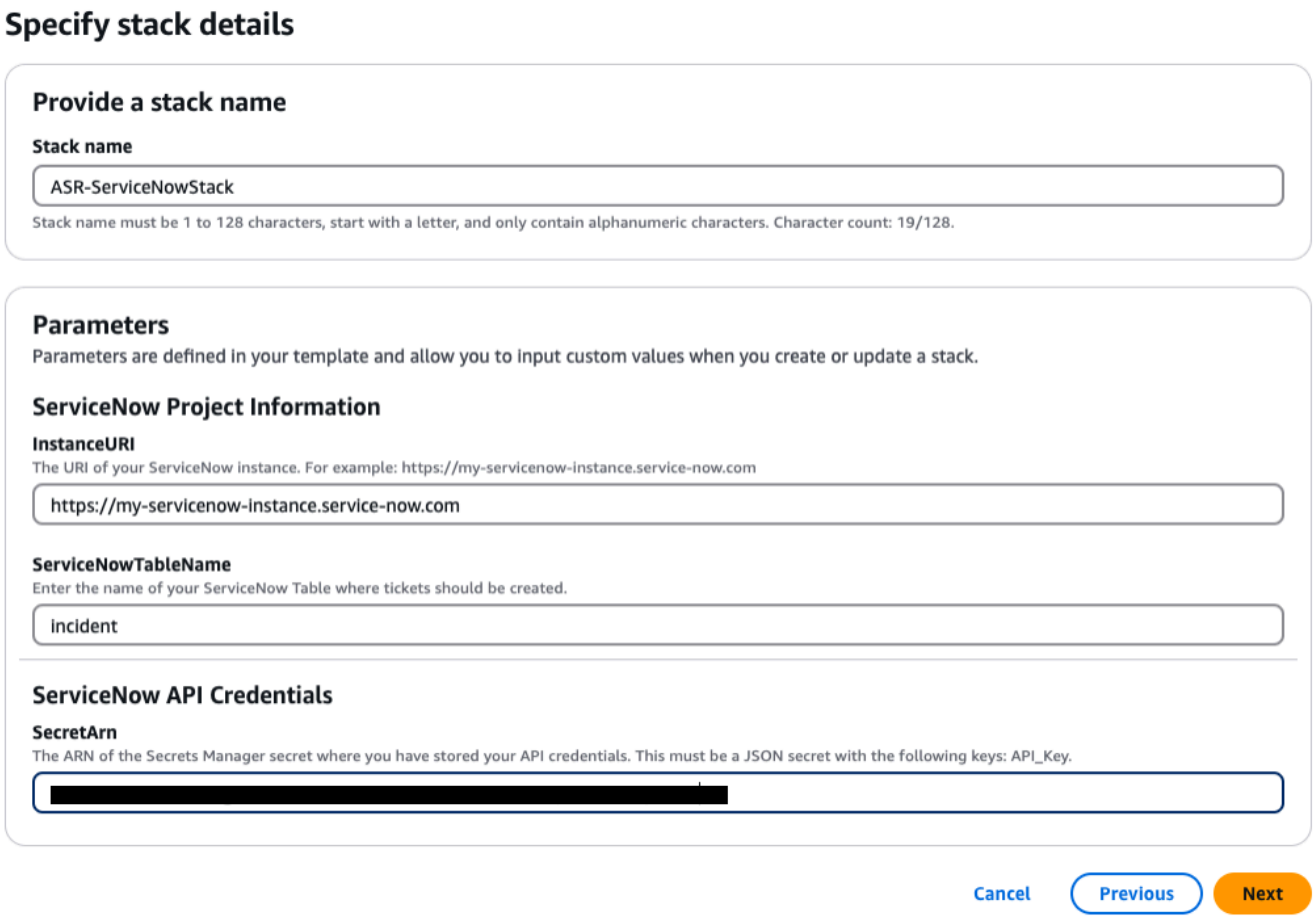
g. Fornisci l'URI della tua ServiceNow istanza.

h. Fornisci il nome della tua ServiceNow tabella.

i. Crea una chiave API ServiceNow con il permesso di modificare la tabella su cui intendi scrivere.

j. Crea un segreto in Secrets Manager con la chiave `API_Key` e fornisci l'ARN segreto come input per lo stack.

Fornisci il nome dello stack, le informazioni sul ServiceNow progetto e le credenziali ServiceNow API.



Per creare uno stack di integrazione personalizzato: includi una funzione Lambda che l'orchestrator della soluzione Step Functions può chiamare per ogni correzione. La funzione

Lambda dovrebbe prendere l'input fornito da Step Functions, creare un payload in base ai requisiti del sistema di ticketing e inviare una richiesta al sistema per creare il ticket.

Passaggio 1: avvia lo stack di amministrazione

> **Important**
>
> Questa soluzione include la raccolta dei dati. Utilizziamo questi dati per comprendere meglio come i clienti utilizzano questa soluzione e i servizi e i prodotti correlati. AWS possiede i dati raccolti tramite questo sondaggio. La raccolta dei dati è soggetta all'Informativa sulla privacy di AWS.

Questo CloudFormation modello AWS automatizzato implementa la soluzione Automated Security Response on AWS nel cloud AWS. Prima di avviare lo stack, devi abilitare Security Hub e completare i prerequisiti.

> **Note**
>
> Sei responsabile del costo dei servizi AWS utilizzati durante l'esecuzione di questa soluzione. Per maggiori dettagli, consulta la sezione Costi di questa guida e consulta la pagina web dei prezzi per ogni servizio AWS utilizzato in questa soluzione.

1. Accedi alla Console di gestione AWS dall'account in cui è attualmente configurato AWS Security Hub e scegli il pulsante qui sotto per avviare il CloudFormation modello `automated-security-response-admin.template` AWS.

   Launch solution

   Puoi anche scaricare il modello come punto di partenza per un'implementazione personalizzata.

2. Per impostazione predefinita, il modello viene avviato nella regione Stati Uniti orientali (Virginia settentrionale). Per avviare questa soluzione in una regione AWS diversa, utilizza il selettore di regione nella barra di navigazione della Console di gestione AWS.

> **Note**
>
> Questa soluzione utilizza AWS Systems Manager, attualmente disponibile solo in specifiche regioni AWS. La soluzione funziona in tutte le regioni che supportano questo servizio. Per la disponibilità più aggiornata per regione, consulta l'elenco dei servizi regionali AWS.

3. Nella pagina Create stack, verifica che l'URL del modello corretto sia nella casella di testo URL di Amazon S3, quindi scegli Avanti.
4. Nella pagina Specifica i dettagli dello stack, assegna un nome allo stack di soluzioni. Per informazioni sulle limitazioni di denominazione dei caratteri, consulta i limiti IAM e STS nella AWS Identity and Access Management User Guide.
5. Nella pagina Parametri, scegli Avanti.

Parametro	Predefinita	Description
Carica SC Admin Stack	`yes`	Specifica se installare i componenti di amministrazione per la correzione automatica dei controlli SC.
Carica AFSBP Admin Stack	no	Specifica se installare i componenti di amministrazione per la correzione automatica dei controlli FSBP.
Carica CIS120 Admin Stack	no	Specifica se installare i componenti di amministrazione per la correzione automatica dei controlli CIS120.
Carica CIS140 Admin Stack	no	Specifica se installare i componenti di amministrazione per la correzion

Parametro	Predefinita	Description
		e automatica dei controlli CIS140.
Carica CIS300 Admin Stack	no	Specifica se installare i componenti di amministr azione per la correzion e automatica dei controlli CIS300.
Carica lo stack di amministr azione PCI321	no	Specifica se installare i componenti di amministr azione per la correzion e automatica dei controlli PCI321.
Carica NIST Admin Stack	no	Specifica se installare i componenti di amministr azione per la correzione automatica dei controlli NIST.

Parametro	Predefinita	Description
Riutilizza Orchestrator Log Group	no	Seleziona se riutilizzare o meno un gruppo di log esistente. `SO0111-ASR-Orchestrator` CloudWatch Ciò semplifica la reinstallazione e gli aggiornamenti senza perdere i dati di registro di una versione precedente. Riutilizza quelli esistenti, `Orchestrator Log Group` scegli `yes` se `Orchestrator Log Group` sono ancora presenti in una distribuzione precedente in questo account, altrimenti. `no` Se stai eseguendo un aggiornamento dello stack da una versione precedente alla v2.3.0, scegli `no`
ShouldDeployWebUI	`yes`	Implementa i componenti dell'interfaccia utente Web tra cui API Gateway, funzioni Lambda e distribuzione. CloudFront Scegli «sì» per abilitare l'interfaccia utente basata sul Web per la visualizzazione dei risultati e dello stato della correzione.

Parametro	Predefinita	Description
AdminUserEmail	(Inserimento opzionale)	Indirizzo email dell'uten te amministratore iniziale. Questo utente avrà accesso amministrativo completo all'interfaccia utente Web ASR. Richiesto solo quando l'interfaccia utente Web è abilitata.
Usa le CloudWatch metriche	`yes`	Specifica se abilitare le CloudWatch metriche per il monitoraggio della soluzione . Verrà creata una CloudWatc h dashboard per la visualizz azione delle metriche.
Usa le CloudWatch metriche e gli allarmi	`yes`	Specifica se abilitare gli allarmi CloudWatch metrici per la soluzione. Questo creerà allarmi per determina te metriche raccolte dalla soluzione.

Parametro	Predefinita	Description
RemediationFailure AlarmThreshold	5	Specifica la soglia per la percentuale di errori di riparazione per ID di controllo . Ad esempio, se si immette5, si riceve un avviso se un ID di controllo non supera più del 5% delle correzioni in un determinato giorno. Questo parametro funziona solo se vengono creati allarmi (vedi il parametro Use CloudWatch Metrics Alarms).
EnableEnhancedClou dWatchMetrics	no	Seyes, crea CloudWatc h metriche aggiuntive per tenere traccia di tutti gli ID di controllo singolarmente sulla CloudWatch dashboard e come allarmi. CloudWatch Consulta la sezione Costo per comprendere i costi aggiuntivi che ciò comporta.
TicketGenFunctionName	(Inserimento opzionale)	Opzionale. Lascia vuoto se non desideri integrare un sistema di biglietteria. Altrimenti, fornisci il nome della funzione Lambda dall'output dello stack di Step 0, ad esempio:. `SO0111-AS R-ServiceNow-Ticke tGenerator`

> **Note**
>
> È necessario abilitare manualmente le correzioni automatiche nell'account Admin dopo aver distribuito o aggiornato gli stack della soluzione. CloudFormation

1. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
2. Nella pagina Rivedi, verifica e conferma le impostazioni. Seleziona la casella che conferma che il modello creerà risorse AWS Identity and Access Management (IAM).
3. Seleziona Create (Crea) per implementare lo stack.

Puoi visualizzare lo stato dello stack nella CloudFormation console AWS nella colonna Status. Dovresti ricevere lo stato CREATE_COMPLETE in circa 15 minuti.

Passaggio 2: installa i ruoli di correzione in ogni account membro di AWS Security Hub

`automated-security-response-member-roles.template` StackSet Devono essere distribuiti in una sola regione per ogni account membro. Definisce i ruoli globali che consentono le chiamate API tra più account dalla funzione step di ASR Orchestrator.

1. Accedi alla Console di gestione AWS per ogni account membro di AWS Security Hub (incluso l'account amministratore, anch'esso membro). Scegli il pulsante per avviare il CloudFormation modello `automated-security-response-member-roles.template` AWS. Puoi anche scaricare il modello come punto di partenza per un'implementazione personalizzata.

2. Per impostazione predefinita, il modello viene avviato nella regione Stati Uniti orientali (Virginia settentrionale). Per avviare questa soluzione in una regione AWS diversa, utilizza il selettore di regione nella barra di navigazione della Console di gestione AWS.
3. Nella pagina Create stack, verifica che l'URL del modello corretto sia nella casella di testo URL di Amazon S3, quindi scegli Avanti.
4. Nella pagina Specifica i dettagli dello stack, assegna un nome allo stack di soluzioni. Per informazioni sulle limitazioni di denominazione dei caratteri, consulta i limiti IAM e STS nella AWS Identity and Access Management User Guide.

5. Nella pagina Parametri, specifica i seguenti parametri e scegli Avanti.

Parametro	Predefinita	Description
Spazio dei nomi	*<Requires input>*	Immettete una stringa composta da un massimo di 9 caratteri alfanumer ici minuscoli. Namespace univoco da aggiungere come suffisso ai nomi dei ruoli IAM di Remediation. Lo stesso namespace deve essere utilizzato nei ruoli dei membri e negli stack dei membri. Questa stringa deve essere univoca per ogni distribuz ione della soluzione, ma non deve essere modificat a durante gli aggiornamenti dello stack. Non è necessari o che il valore dello spazio dei nomi sia univoco per account membro.
Account amministratore Sec Hub	*<Requires input>*	Inserisci l'ID dell'account di 12 cifre per l'account amministratore di AWS Security Hub. Questo valore concede le autorizzazioni per il ruolo di soluzione dell'acco unt amministratore.

6. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
7. Nella pagina Rivedi, verifica e conferma le impostazioni. Seleziona la casella che conferma che il modello creerà risorse AWS Identity and Access Management (IAM).
8. Seleziona Create (Crea) per implementare lo stack.

Puoi visualizzare lo stato dello stack nella CloudFormation console AWS nella colonna Status. Dovresti ricevere lo stato CREATE_COMPLETE in circa 5 minuti. Puoi continuare con il passaggio successivo mentre questo stack viene caricato.

Fase 3: Avvia lo stack di membri

> **Important**
>
> Questa soluzione include la raccolta dei dati. Utilizziamo questi dati per comprendere meglio come i clienti utilizzano questa soluzione e i servizi e i prodotti correlati. AWS è proprietaria dei dati raccolti tramite questo sondaggio. La raccolta dei dati è soggetta all'Informativa sulla privacy di AWS.

Lo `automated-security-response-member` stack deve essere installato in ogni account membro di Security Hub. Questo stack definisce i runbook per la correzione automatica. L'amministratore di ogni account membro può controllare quali correzioni sono disponibili tramite questo stack.

1. Accedi alla Console di gestione AWS per ogni account membro di AWS Security Hub (incluso l'account amministratore, anch'esso membro). Scegli il pulsante per avviare il CloudFormation modello `automated-security-response-member.template` AWS.

   Launch solution

Puoi anche scaricare il modello come punto di partenza per la tua implementazione. Per impostazione predefinita, il modello viene avviato nella regione Stati Uniti orientali (Virginia settentrionale). Per avviare questa soluzione in una regione AWS diversa, utilizza il selettore di regione nella barra di navigazione della Console di gestione AWS.

+

> **Note**
>
> Questa soluzione utilizza AWS Systems Manager, attualmente disponibile nella maggior parte delle regioni AWS. La soluzione funziona in tutte le regioni che supportano questi

servizi. Per la disponibilità più aggiornata per regione, consulta l'elenco dei servizi regionali AWS.

1. Nella pagina Create stack, verifica che l'URL del modello corretto sia nella casella di testo URL di Amazon S3, quindi scegli Avanti.
2. Nella pagina Specifica i dettagli dello stack, assegna un nome allo stack di soluzioni. Per informazioni sulle limitazioni di denominazione dei caratteri, consulta i limiti IAM e STS nella AWS Identity and Access Management User Guide.
3. Nella pagina Parametri, specifica i seguenti parametri e scegli Avanti.

Parametro	Predefinita	Description
Fornite il nome LogGroup da utilizzare per creare filtri metrici e allarmi	*<Requires input>*	Specifica il nome di un gruppo di CloudWatch CloudTrail log in cui vengono registrate le chiamate API. Viene utilizzato per le correzioni CIS 3.1-3.14.
Carica SC Member Stack	yes	Specifica se installare i componenti dei membri per la correzione automatica dei controlli SC.
Carica AFSBP Member Stack	no	Specifica se installare i componenti dei membri per la correzione automatica dei controlli FSBP.
Carica lo stack di membri CIS120	no	Specificare se installare i componenti membri per la riparazione automatica dei controlli CIS120.
Carica lo stack di membri CIS140	no	Specificare se installare i componenti membri per la

Parametro	Predefinita	Description
		riparazione automatica dei controlli CIS140.
Carica lo stack di membri CIS300	no	Specifica se installare i componenti membri per la correzione automatica dei controlli CIS300.
Carica PCI321 Member Stack	no	Specifica se installare i componenti membri per la correzione automatica dei controlli PCI321.
Carica NIST Member Stack	no	Specifica se installare i componenti dei membri per la correzione automatica dei controlli NIST.
Crea un bucket S3 per Redshift Audit Logging	no	Scegli `yes` di creare il bucket S3 per la correzione FSBP. RedShift.4 Per i dettagli sul bucket S3 e sulla correzione, consulta la correzione nella Guida per l'utente di AWS Security Redshift.4 Hub.
Account amministratore Sec Hub	*<Requires input>*	Inserisci l'ID dell'account di 12 cifre per l'account amministratore di AWS Security Hub.

Parametro	Predefinita	Description
Spazio dei nomi	`<Requires input>`	Inserisci una stringa composta da un massimo di 9 caratteri alfanumerici minuscoli. Questa stringa diventa parte dei nomi dei ruoli IAM e del bucket Action Log S3. Utilizza lo stesso valore per la distribuzione dello stack dei membri e per la distribuzione dello stack dei ruoli dei membri. La stringa deve essere univoca per ogni distribuzione della soluzione, ma non deve essere modificata durante gli aggiornamenti dello stack.

Parametro	Predefinita	Description
EnableCloudTrailForASRActionLog	no	Seleziona `yes` se desideri monitorare gli eventi di gestione condotti dalla soluzione sulla CloudWatch dashboard. La soluzione crea un CloudTrail percorso nell'account di ogni membro selezionato`yes`. È necessario distribuire la soluzione in un'organizzazione AWS per abilitare questa funzionalità. Inoltre, puoi abilitare questa funzionalità solo in una singola regione all'interno dello stesso account. Consulta la sezione Costo per comprendere i costi aggiuntivi che ciò comporta.

4. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
5. Nella pagina Rivedi, verifica e conferma le impostazioni. Seleziona la casella che conferma che il modello creerà risorse AWS Identity and Access Management (IAM).
6. Seleziona Create (Crea) per implementare lo stack.

Puoi visualizzare lo stato dello stack nella CloudFormation console AWS nella colonna Status. Dovresti ricevere lo stato CREATE_COMPLETE in circa 15 minuti.

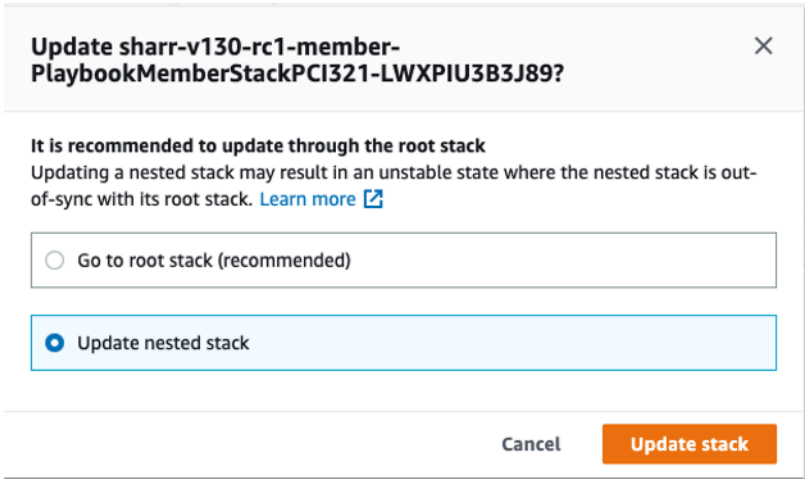
Fase 4: (Facoltativo) Modifica le correzioni disponibili

Se desideri rimuovere correzioni specifiche da un account membro, puoi farlo aggiornando lo stack annidato per lo standard di sicurezza. Per semplicità, le opzioni dello stack annidato non vengono propagate allo stack principale.

1. Accedi alla CloudFormation console AWS e seleziona lo stack annidato.
2. Scegliere Aggiorna.

3. Seleziona Aggiorna stack annidato e scegli Update stack.

   Aggiorna lo stack annidato



4. Seleziona Usa il modello corrente e scegli Avanti.
5. Modifica le correzioni disponibili. Cambia i valori per i controlli desiderati `Available` e per i controlli indesiderati in. `Not available`

> **Note**
>
> La disattivazione di una correzione rimuove il runbook di correzione della soluzione per lo standard e il controllo di sicurezza.

6. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
7. Nella pagina Rivedi, verifica e conferma le impostazioni. Seleziona la casella che conferma che il modello creerà risorse AWS Identity and Access Management (IAM).
8. Scegli Aggiorna stack.

Puoi visualizzare lo stato dello stack nella CloudFormation console AWS nella colonna Status. Dovresti ricevere lo stato CREATE_COMPLETE in circa 15 minuti.

Distribuzione di AWS Control Tower (CT)

La guida Customizations for AWS Control Tower (cFCT) è rivolta ad amministratori, DevOps professionisti, fornitori di software indipendenti, architetti di infrastrutture IT e integratori di sistemi che desiderano personalizzare ed estendere i propri ambienti AWS Control Tower per la propria azienda

e i propri clienti. Fornisce informazioni sulla personalizzazione e l'estensione dell'ambiente AWS Control Tower con il pacchetto di personalizzazione cFCT.

Tempo di distribuzione: circa 30 minuti

Prerequisiti

Prima di distribuire questa soluzione, assicurati che sia destinata agli amministratori di AWS Control Tower.

Quando sei pronto per configurare la tua zona di destinazione utilizzando la console o le API di AWS Control Tower, segui questi passaggi:

Per iniziare a usare AWS Control Tower, consulta: Guida introduttiva ad AWS Control Tower

Per informazioni su come personalizzare la zona di atterraggio, consulta: Personalizzazione della zona di atterraggio

Per avviare e implementare la tua zona di atterraggio, consulta: Landing Zone Deployment Guide

Panoramica sull'implementazione

Utilizza i seguenti passaggi per distribuire questa soluzione su AWS.

Passaggio 1: crea e distribuisci un bucket S3

> **Note**
>
> Configurazione del bucket S3: solo per ADMIN. Questa è una fase di configurazione unica e non deve essere ripetuta dagli utenti finali. I bucket S3 memorizzano il pacchetto di distribuzione, incluso il CloudFormation modello AWS e il codice Lambda necessari per l'esecuzione di ASR. Queste risorse vengono distribuite utilizzando o. CfCt StackSet

1. Configura il bucket S3

Configura il bucket S3 che verrà utilizzato per archiviare e gestire i pacchetti di distribuzione.

2. Configurazione dell'ambiente

Prepara le variabili di ambiente, le credenziali e gli strumenti necessari per il processo di creazione e distribuzione.

3. Configura le politiche del bucket S3

Definisci e applica le politiche dei bucket appropriate per controllare gli accessi e le autorizzazioni.

4. Prepara la build

Compilate, impacchettate o preparate in altro modo l'applicazione o le risorse per la distribuzione.

5. Distribuisci i pacchetti su S3

Carica gli artefatti di compilazione preparati nel bucket S3 designato.

Fase 2: distribuzione degli stack su AWS Control Tower

1. Crea un Build Manifest per i componenti ASR

Definisci un manifesto di compilazione che elenca tutti i componenti ASR, le relative versioni, dipendenze e istruzioni di compilazione.

2. Aggiorna il CodePipeline

Modifica la CodePipeline configurazione AWS per includere le nuove fasi di compilazione, gli artefatti o le fasi necessari per la distribuzione dei componenti ASR.

Fase 1: creazione e distribuzione nel bucket S3

Le soluzioni AWS utilizzano due bucket: un bucket per l'accesso globale ai modelli, a cui si accede tramite HTTPS, e bucket regionali per l'accesso alle risorse all'interno della regione, come il codice Lambda.

1. Configura il bucket S3

Scegli un nome univoco per il bucket, ad esempio asr-staging. Imposta due variabili di ambiente sul tuo terminale, una dovrebbe essere il nome del bucket di base con -reference come suffisso, l'altra con la regione di distribuzione prevista come suffisso:

```
export BASE_BUCKET_NAME=asr-staging-$(date +%s)
export TEMPLATE_BUCKET_NAME=$BASE_BUCKET_NAME-reference
export REGION=us-east-1
export ASSET_BUCKET_NAME=$BASE_BUCKET_NAME-$REGION
```

2. Configurazione dell'ambiente

Nel tuo account AWS, crea due bucket con questi nomi, ad esempio asr-staging-reference e asr-staging-us-east-1. (Il bucket di riferimento conterrà i CloudFormation modelli, il bucket regionale conterrà tutte le altre risorse come il pacchetto di codice lambda.) I tuoi bucket devono essere crittografati e non devono consentire l'accesso pubblico

```
aws s3 mb s3://$TEMPLATE_BUCKET_NAME/
aws s3 mb s3://$ASSET_BUCKET_NAME/
```

> **Note**
>
> Quando crei i bucket, assicurati che non siano accessibili al pubblico. Usa nomi di bucket casuali. Disabilita l'accesso pubblico. Usa la crittografia KMS. E verifica la proprietà del bucket prima del caricamento.

3. Configurazione della politica dei bucket S3

Aggiorna la policy del bucket S3 $TEMPLATE_BUCKET_NAME per includere le autorizzazioni per l'ID dell'account di esecuzione. PutObject Assegna questa autorizzazione a un ruolo IAM all'interno dell'account di esecuzione autorizzato a scrivere nel bucket. Questa configurazione consente di evitare di creare il bucket nell'account di gestione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::template-bucket-name/*",
                "arn:aws:s3:::template-bucket-name"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "org-id"
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::template-bucket-name/*",
                "arn:aws:s3:::template-bucket-name"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::account-id:role/iam-role-name"
                }
            }
        }
    ]
}
```

Modifica la policy del bucket S3 dell'asset per includere le autorizzazioni. Assegna questa autorizzazione a un ruolo IAM all'interno dell'account di esecuzione autorizzato a scrivere nel bucket. Ripeti questa configurazione per ogni bucket di risorse regionale (ad esempio, asr-staging-us-east-1, asr-staging-eu-west-1 e così via), consentendo le distribuzioni in più regioni senza dover creare i bucket nell'account di gestione.

4. Preparazione della build

- Prerequisiti:
  - AWS CLI v2
  - Python 3.11+ con pip
  - ERA CDK 2.17.11+
  - Node.js 22+ con npm
  - Poetry v2 con plugin per esportare
- Git clone automated-security-response-on-aws repository GitHub

Per prima cosa assicurati di aver eseguito npm install nella cartella dei sorgenti.

Successivamente, dalla cartella di distribuzione del repository clonato, esegui build-s3-dist.sh, passando il nome principale del bucket (ad esempio, mybucket) e la versione che stai creando (ad esempio, v1.0.0). Usa una versione semver basata sulla versione scaricata da GitHub (ad esempio,: v1.0.0, la tua build: v1.0.0.mybuild). GitHub

```
chmod +x build-s3-dist.sh
```

```
export SOLUTION_NAME=automated-security-response-on-aws
export SOLUTION_VERSION=v1.0.0.mybuild
./build-s3-dist.sh -b $BASE_BUCKET_NAME -v $SOLUTION_VERSION
```

5. Distribuisci pacchetti su S3

```
cd deployment
aws s3 cp global-s3-assets/  s3://$TEMPLATE_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive
aws s3 cp regional-s3-assets/  s3://$ASSET_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive
```

Fase 2: distribuzione degli stack su AWS Control Tower

1. Crea un manifesto per i componenti ASR

Dopo aver distribuito gli artefatti ASR nei bucket S3, aggiorna il manifesto della pipeline di AWS Control Tower in modo che faccia riferimento alla nuova versione, quindi attiva l'esecuzione della pipeline. Per ulteriori informazioni, consulta la distribuzione di AWS Control Tower. https://docs.aws.amazon.com/controltower/latest/userguide/deployment.html

> **Important**
>
> Per una corretta distribuzione della soluzione ASR, consulta la documentazione ufficiale di AWS per informazioni dettagliate sulla panoramica dei CloudFormation modelli e sulla descrizione dei parametri. Di seguito sono riportati i link informativi: Guida alla panoramica CloudFormation dei parametri dei modelli

Il manifesto dei componenti ASR ha il seguente aspetto:

```
region: us-east-1 #<HOME_REGION_NAME>
version: 2021-03-15

# Control Tower Custom CloudFormation Resources
resources:
  - name: <ADMIN STACK NAME>
    resource_file: s3://<ADMIN TEMPLATE BUCKET path>
    parameters:
      - parameter_key: UseCloudWatchMetricsAlarms
        parameter_value: "yes"
```

```
      - parameter_key: TicketGenFunctionName
        parameter_value: ""
      - parameter_key: ShouldDeployWebUI
        parameter_value: "yes"
      - parameter_key: AdminUserEmail
        parameter_value: "<YOUR EMAIL ADDRESS>"
      - parameter_key: LoadSCAdminStack
        parameter_value: "yes"
      - parameter_key: LoadCIS120AdminStack
        parameter_value: "no"
      - parameter_key: LoadCIS300AdminStack
        parameter_value: "no"
      - parameter_key: UseCloudWatchMetrics
        parameter_value: "yes"
      - parameter_key: LoadNIST80053AdminStack
        parameter_value: "no"
      - parameter_key: LoadCIS140AdminStack
        parameter_value: "no"
      - parameter_key: ReuseOrchestratorLogGroup
        parameter_value: "yes"
      - parameter_key: LoadPCI321AdminStack
        parameter_value: "no"
      - parameter_key: RemediationFailureAlarmThreshold
        parameter_value: "5"
      - parameter_key: LoadAFSBPAdminStack
        parameter_value: "no"
      - parameter_key: EnableEnhancedCloudWatchMetrics
        parameter_value: "no"
    deploy_method: stack_set
    deployment_targets:
     accounts: # :type: list
        - <ACCOUNT_NAME> # and/or
        - <ACCOUNT_NUMBER>
    regions:
      - <REGION_NAME>

  - name:  <ROLE MEMBER STACK NAME>
    resource_file: s3://<ROLE MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: Namespace
        parameter_value: <NAMESPACE>
    deploy_method: stack_set
```

```
    deployment_targets:
      organizational_units:
        - <ORG UNIT>

  - name:  <MEMBER STACK NAME>
    resource_file: s3://<MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: LoadCIS120MemberStack
        parameter_value: "no"
      - parameter_key: LoadNIST80053MemberStack
        parameter_value: "no"
      - parameter_key: Namespace
        parameter_value: <NAMESPACE>
      - parameter_key: CreateS3BucketForRedshiftAuditLogging
        parameter_value: "no"
      - parameter_key: LoadAFSBPMemberStack
        parameter_value: "no"
      - parameter_key: LoadSCMemberStack
        parameter_value: "yes"
      - parameter_key: LoadPCI321MemberStack
        parameter_value: "no"
      - parameter_key: LoadCIS140MemberStack
        parameter_value: "no"
      - parameter_key: EnableCloudTrailForASRActionLog
        parameter_value: "no"
      - parameter_key: LogGroupName
        parameter_value: <LOG_GROUP_NAME>
      - parameter_key: LoadCIS300MemberStack
        parameter_value: "no"
    deploy_method: stack_set
    deployment_targets:
      accounts: # :type: list
        - <ACCOUNT_NAME> # and/or
        - <ACCOUNT_NUMBER>
      organizational_units:
        - <ORG UNIT>
    regions: # :type: list
      - <REGION_NAME>
```

2. Aggiornamento della pipeline di codice

Aggiungi un file manifest a un file custom-control-tower-configuration.zip ed esegui un CodePipeline, vedi: panoramica della pipeline di codice

Puoi verificare la distribuzione controllando lo stato della pipeline di AWS Control Tower nella console AWS. CodePipeline

Utilizzo programmatico dell'API ASR

Se desideri integrare l'ASR nei tuoi sistemi, ad esempio una piattaforma di orchestrazione della sicurezza, un ticketing o un ChatOps flusso di lavoro o una dashboard personalizzata e avviare le correzioni da lì anziché dall'interfaccia utente Web, puoi chiamare direttamente l'API Automated Security Response on AWS (ASR). Con l'API ASR, puoi automatizzare e monitorare le correzioni degli strumenti che già utilizzi.

A tale scopo, utilizzate un client machine-to-machine (M2M) con la concessione OAuth 2.0. `client_credentials` Quando l'interfaccia utente Web è abilitata, la soluzione fornisce l'ambito OAuth di Amazon Cognito. `asr-api/full-access` Questo ambito garantisce al client l'accesso all'API ASR. Il client dell'app M2M viene creato personalmente dopo la distribuzione. La soluzione non ne crea una, quindi non esiste alcuna credenziale del computer finché non effettui l'attivazione.

Un token con questo `asr-api/full-access` ambito ha l'accesso completo, la stessa funzionalità del ruolo di amministratore della soluzione, inclusa la possibilità di gestire altri utenti. Tratta le credenziali con la stessa cura delle credenziali di accesso dell'amministratore.

Prerequisiti

Implementa lo stack di amministratori ASR con l'interfaccia utente Web abilitata (impostazione predefinita)`ShouldDeployWebUI=yes`. Questo crea il pool di utenti di Amazon Cognito, l'API e l'ambito. `asr-api/full-access` È inoltre necessario:

- AWS CLI v2 autenticata con l'account amministratore ASR
- `curle jq` per gli esempi di token e API riportati di seguito

Passaggio 1: creare il client dell'app M2M dopo la distribuzione

Trova l'ID del pool di utenti nell'`UserPoolId`Output dello stack di amministratori, quindi crea un client riservato con entrambi gli ambiti OAuth 2.0 richiesti `asr-api/api` (Amazon API Gateway richiede

questo ambito per ammettere la richiesta all'API) e `asr-api/full-access` (il backend autorizza l'accesso completo a questo ambito). Un client concesso `asr-api/api` raggiunge solo l'API ma riceve un `403` rifiuto, perché il backend lo considera un token macchina non privilegiato.

```
export AWS_REGION="us-east-1"
export STACK_NAME="<ASR-administrator-stack-name>"

export USER_POOL_ID="$(aws cloudformation describe-stacks \
  --stack-name "$STACK_NAME" --region "$AWS_REGION" \
  --query "Stacks[0].Outputs[?OutputKey=='UserPoolId'].OutputValue" --output text)"

CREATE_OUT="$(aws cognito-idp create-user-pool-client \
  --user-pool-id "$USER_POOL_ID" --region "$AWS_REGION" \
  --client-name "ASR-M2M-FullAccess" \
  --generate-secret \
  --allowed-o-auth-flows client_credentials \
  --allowed-o-auth-flows-user-pool-client \
  --allowed-o-auth-scopes "asr-api/api" "asr-api/full-access" \
  --output json)"

export M2M_CLIENT_ID="$(echo "$CREATE_OUT" | jq -r '.UserPoolClient.ClientId')"
export CLIENT_SECRET="$(echo "$CREATE_OUT" | jq -r '.UserPoolClient.ClientSecret')"
```

La risposta contiene e. `UserPoolClient.ClientId` `UserPoolClient.ClientSecret` Cognito ti mostra il valore segreto solo una volta. Cognito richiede che il segreto venga generato al momento della creazione del client (`--generate-secret`); non esiste alcun comando per aggiungere un segreto a un client esistente in un secondo momento.

Fase 2: Archivia il segreto nel tuo negozio segreto

La soluzione non memorizza mai questo segreto. Viene intenzionalmente tenuto fuori dagli CloudFormation output di AWS e dallo stato del modello. Sei responsabile dell'acquisizione del segreto del cliente restituito e della sua archiviazione sicura nel tuo archivio segreto, ad esempio AWS Secrets Manager, AWS Systems Manager Parameter Store (Secure String) o il vault della tua organizzazione.

- Archivia il segreto immediatamente; non puoi recuperarlo nuovamente in seguito.
- Limita l'accesso in lettura all'integrazione che ne ha bisogno.
- Chiunque detenga questo segreto può ottenere i token di accesso completo per ASR, quindi proteggili di conseguenza.

Fase 3: Recupera un token di accesso (client_credentials flow)

L'endpoint del token è derivato dal dominio ospitato del pool di utenti. Richiedi un token utilizzando HTTP Basic auth (`client_id:client_secret`), la `client_credentials` concessione ed entrambi gli ambiti:

```
export DOMAIN_PREFIX="$(aws cognito-idp describe-user-pool \
  --user-pool-id "$USER_POOL_ID" --region "$AWS_REGION" \
  --query "UserPool.Domain" --output text)"
export TOKEN_URL="https://${DOMAIN_PREFIX}.auth.${AWS_REGION}.amazoncognito.com/oauth2/
token"

export ACCESS_TOKEN="$(curl -s -X POST "$TOKEN_URL" \
  -H "Content-Type: application/x-www-form-urlencoded" \
  -u "${M2M_CLIENT_ID}:${CLIENT_SECRET}" \
  -d "grant_type=client_credentials&scope=asr-api/api asr-api/full-access" \
  | jq -r '.access_token')"
```

I token di accesso sono validi per 1 ora e la `client_credentials` concessione non emette un token di aggiornamento. Memorizza e riutilizza un token per tutta la durata della sua validità anziché richiederne uno nuovo per ogni chiamata API. Richiedi un nuovo token poco prima della scadenza di quello attuale, ad esempio uno o due minuti prima dell'ora, utilizzando le credenziali che già possiedi.

La memorizzazione nella cache del token mantiene l'integrazione entro i limiti di velocità degli endpoint del token Cognito e riduce i costi. Una corretta integrazione nella cache richiede solo una richiesta di token all'ora. La richiesta di un nuovo token per ogni chiamata API è più lenta e inutilmente costosa.

Fase 4: Chiama l'API ASR

Invia il token di accesso come `Authorization: Bearer <access_token>` intestazione su qualsiasi percorso dell'API ASR. API Gateway convalida il token e l'`asr-api/api`ambito prima che la richiesta raggiunga il backend e il backend concede l'accesso completo all'ambito: `asr-api/full-access`

```
# Find the API base URL in the administrator stack's APIEndpoint Output, then
# call an endpoint your integration uses.
curl -s -H "Authorization: Bearer ${ACCESS_TOKEN}" \
  "https://<api-id>.execute-api.${AWS_REGION}.amazonaws.com/prod/<endpoint>"
```

Non è necessaria una configurazione aggiuntiva di rete o firewall per i chiamanti programmatici. Le protezioni AWS WAF dell'API ammettono già client di macchine autenticati (agenti utente non browser provenienti da intervalli IP cloud) bloccando al contempo il traffico abusivo. L'attività della macchina viene attribuita all'ID del cliente nei log dell'API ASR e AWS registra ogni emissione di token. CloudTrail

Fase 5: Ruota o disabilita il client

Poiché un segreto non può essere aggiunto, sostituito o rimosso su un client dell'app Cognito esistente, la rotazione e la disabilitazione avvengono sul client stesso:

- Ruota: crea un secondo client M2M (ripeti il passaggio 1 con un altro`--client-name`), migra l'integrazione alle relative credenziali, conferma che possa ottenere i token, quindi elimina il vecchio client.
- Disabilita: elimina il client per revocare immediatamente l'accesso alla macchina.

```
aws cognito-idp delete-user-pool-client \
  --user-pool-id "$USER_POOL_ID" \
  --client-id "$M2M_CLIENT_ID" \
  --region "$AWS_REGION"
```

Rileva i token del computer negati (opzionale)

Quando gli CloudWatch allarmi Amazon sono abilitati, ASR invia un avviso opt-in (`ASR-Cognito-M2MForbidden`) sulla metrica. `ASR/M2MForbiddenAuthorization` La funzione API AWS Lambda emette questa metrica ogni volta che un token di macchina viene negato perché privo dell'`asr-api/full-access`ambito: un conteggio diverso da zero segnala un client o un sondaggio non configurati correttamente. L'allarme utilizza l'argomento di allarme SNS condiviso da ASR, che per impostazione predefinita non ha abbonati; iscriviti a un canale per ricevere una notifica.

Abilita la registrazione di Amazon Cognito e la protezione dalle minacce

Ti consigliamo di abilitare la distribuzione nativa dei log e Advanced Security nel pool di utenti ASR per la visibilità delle attività di autenticazione.

Distribuzione nativa dei log di Amazon Cognito

Con questa opzione, puoi inviare eventi di accesso e token ad Amazon CloudWatch Logs. Nella console Amazon Cognito, apri il tuo pool di utenti e scegli Registrazione. Abilita la consegna dei

log a un gruppo di CloudWatch log Logs. Imposta il livello di registro su `ERROR` o in `INFO` base alla quantità di dettagli di cui hai bisogno.

Amazon Cognito registra l'emissione di token in AWS. CloudTrail Per conservare e interrogare questi record di controllo in Amazon CloudWatch Logs, configura un CloudTrail percorso degli eventi di gestione nell'account proprietario del pool di utenti. Configura il percorso per inviare i log a un gruppo di log CloudWatch Logs. Per ulteriori informazioni, consulta Monitoraggio dei file di CloudTrail log con Amazon CloudWatch Logs.

Amazon Cognito: sicurezza avanzata e protezione dalle minacce

Con questa opzione, ottieni il rilevamento delle credenziali compromesse e l'autenticazione adattiva basata sul rischio. Nella console Amazon Cognito, apri il tuo pool di utenti, scegli Advanced Security e imposta la modalità su Enforced.

> **Costo aggiuntivo**
>
> Se abiliti Advanced Security, dovrai sostenere costi aggiuntivi per autenticazione. Per ulteriori informazioni sui prezzi di Amazon Cognito, consulta i prezzi di Amazon Cognito.

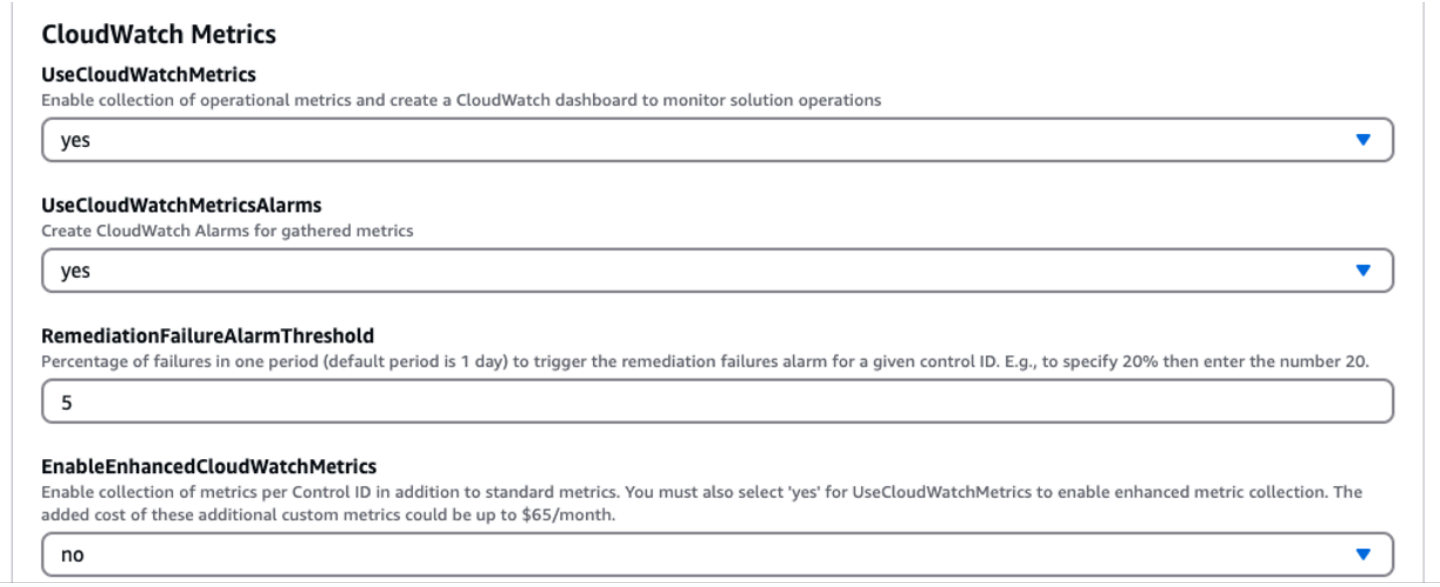
Monitora le operazioni della soluzione con una CloudWatch dashboard Amazon

Questa soluzione include metriche e allarmi personalizzati visualizzati su una dashboard Amazon CloudWatch .

La CloudWatch dashboard e gli allarmi monitorano le operazioni della soluzione e avvisano in caso di potenziale problema.

Abilitazione di CloudWatch metriche, allarmi e dashboard

Esistono quattro parametri del CloudFormation modello per la CloudWatch funzionalità.



1. UseCloudWatchMetrics- L'impostazione di questo valore `yes` consente la raccolta di metriche operative e crea un CloudWatch pannello di controllo per visualizzare tali metriche.
2. UseCloudWatchAlarms- Impostandolo in modo da `yes` abilitare gli allarmi predefiniti della soluzione.
3. RemediationFailureAlarmThreshold- La percentuale di interventi correttivi non riusciti in un periodo per far scattare un allarme.
4. EnableEnhancedCloudWatchMetrics- Imposta questo parametro per `yes` raccogliere le singole metriche per ID di controllo. Per impostazione predefinita, questo parametro è impostato suno, in modo che vengano raccolte solo le metriche sul numero totale di correzioni su tutti gli ID di controllo. Le singole metriche e gli allarmi per ID di controllo comportano costi aggiuntivi.

Utilizzo del pannello di controllo CloudWatch

Per visualizzare il pannello di controllo:

1. Accedi ad Amazon CloudWatch e poi a Dashboards.
2. Seleziona la dashboard denominata "ASR-Remediation-Metrics-Dashboard».

La CloudWatch dashboard contiene le seguenti sezioni:

1. Rimediazioni riuscite in totale: fornisce informazioni dettagliate sul numero di riscontri di Security Hub che sono stati corretti con successo dalla soluzione.
2. Errori di riparazione: mostra quante riparazioni hanno avuto esito negativo, sia in totale che in percentuale, e la causa dell'errore. Un numero elevato di errori può indicare un problema tecnico relativo alla soluzione che potrebbe essere necessario esaminare più dettagliatamente.
3. Correzione Success/Failure tramite Control ID: se hai abilitato Enhanced Metrics al momento della distribuzione, questa sezione elenca i risultati della correzione in base all'ID di controllo. Quando la sezione Errori di riparazione mostra un tasso di errore elevato in generale, questa sezione mostra se gli errori sono distribuiti su molti ID di controllo o se solo alcuni ID di controllo non funzionano.
4. Runbook Assume Role Failures: mostra il numero di errori che si sono verificati a causa di tentativi di correzione negli account in cui non è installato il ruolo di membro della soluzione. Gli errori ripetuti dovuti a tentativi di riparazione automatici dovuti alla mancanza di ruoli comportano costi inutili. Riduci questo problema installando lo stack di ruoli Member negli account interessati, disabilitando tutte le EventBridge regole create dalla soluzione o dissociando l'account in Security Hub.
5. Cloud Trail Management Actions by ASR: elenca le azioni di gestione della soluzione in tutti gli account membri in cui hai abilitato i log delle azioni con il parametro al momento della EnableCloudTrailForASRActionLog distribuzione. Quando osservi cambiamenti imprevisti delle risorse in uno qualsiasi dei tuoi account AWS, questo widget può aiutarti a capire se le risorse sono state modificate dalla soluzione.

La CloudWatch dashboard include anche allarmi predefiniti che segnalano errori operativi comuni.

1. Esecuzioni di State Machine > 1000 in un periodo di 24 ore.
   a. Un forte aumento delle esecuzioni di correzione potrebbe indicare che una regola di evento viene avviata più spesso del previsto.

   b. La soglia può essere modificata utilizzando il parametro. CloudFormation

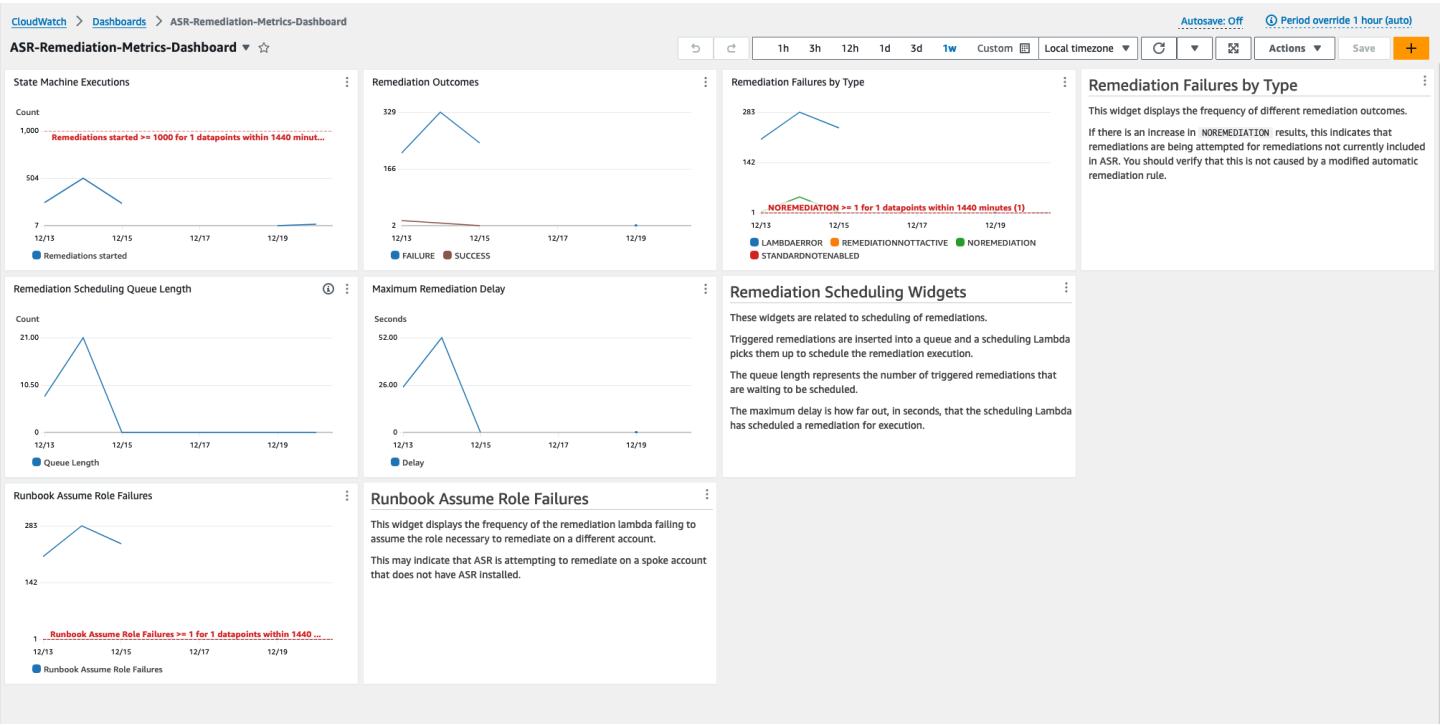
2. Errori di riparazione per tipo = NESSUNA RIPARAZIONE > 0

   a. Si sta tentando di porre rimedio a problemi non inclusi nell'ASR. Ciò potrebbe indicare che una regola di evento è stata modificata per includere più correzioni rispetto a quelle previste.

3. Runbook Assume Role Fallimenti > 0

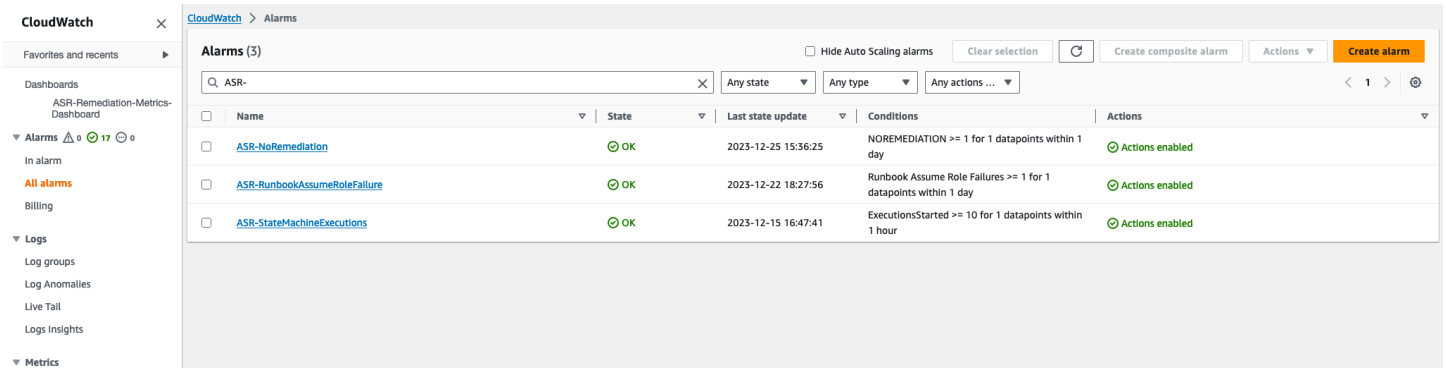
   a. Si stanno tentando di porre rimedio agli account o alle regioni in cui la soluzione non è stata implementata correttamente. Ciò potrebbe indicare che una regola di evento è stata modificata per includere più account del previsto.

Tutte le soglie di allarme possono essere modificate per soddisfare le esigenze di implementazione individuali.

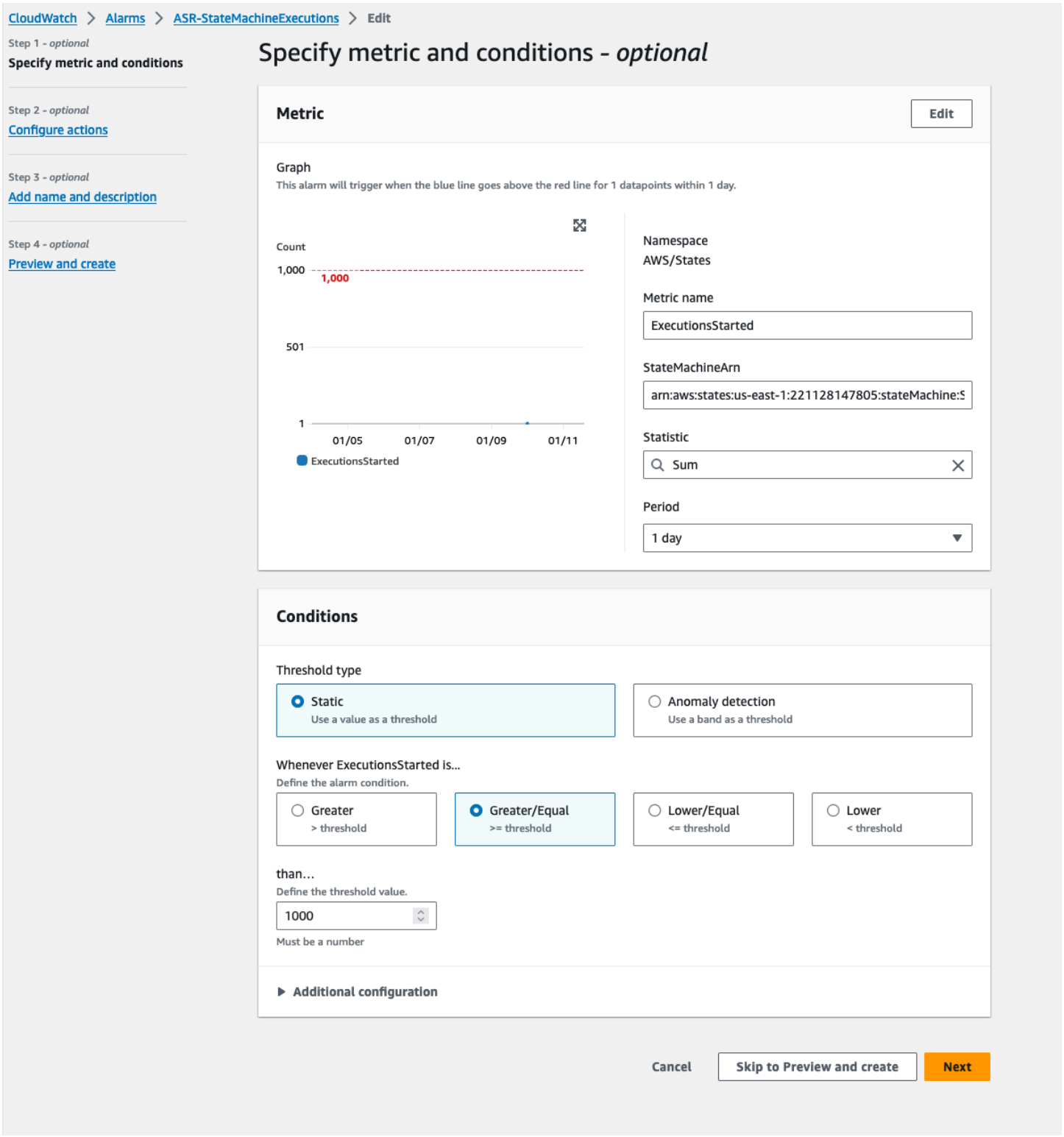


Modifica delle soglie di allarme

1. Accedi ad [Amazon CloudWatch → Allarmi → Tutti gli allarmi.]
2. Scegli l'allarme che desideri modificare, quindi scegli Azioni, quindi scegli Modifica.



1. Cambia la soglia sul valore desiderato e salva.



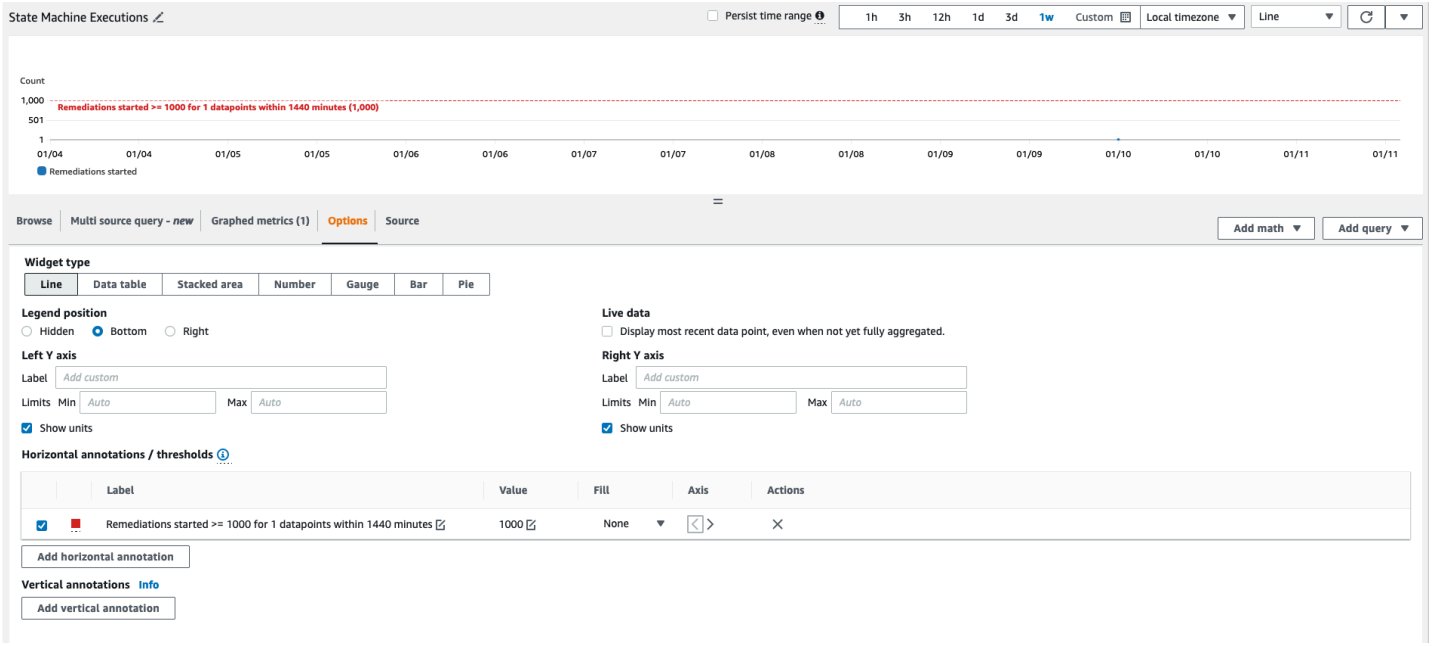
1. Accedi alla CloudWatch dashboard per modificare i grafici in modo che corrispondano alle nuove impostazioni.

   a. Scegli i puntini di sospensione in alto a destra del widget corrispondente.

b. Scegli Modifica.

c. Scegli la scheda Opzioni.

d. Modificate l'annotazione Alarm in modo che corrisponda alle nuove impostazioni.



Iscrizione alle notifiche di allarme

Nell'account amministratore, iscriviti all'argomento Amazon SNS creato dallo stack di amministrazione, SO0111-ASR _. Alarm_Topic Questo ti avviserà quando un allarme entra nello stato ALARM.

Aggiorna la soluzione

Important

- Aggiornamento alla versione 4.0.0 o successiva: la soluzione mantiene le impostazioni di riparazione automatica esistenti durante l'aggiornamento. Se si esegue l'aggiornamento dalla versione 2.x, la soluzione migra automaticamente le impostazioni di correzione automatica dalle regole della versione 2 alla nuova configurazione durante l'aggiornamento dello stack. EventBridge DynamoDB-backed I controlli per i quali avevi abilitato la correzione automatica nella v2 restano abilitati nella v4, mentre i controlli senza un equivalente v3+ vengono ignorati ed elencati nei log Amazon della funzione di migrazione AWS Lambda. CloudWatch Se stai effettuando l'aggiornamento dalla versione 3.x, le impostazioni di riparazione automatica sono già incluse nella configurazione e vengono mantenute invariate, quindi non è necessaria alcuna migrazione. DynamoDB-backed Se la migrazione rileva un errore per controllo o si interrompe prima della scrittura dei controlli, la funzione Lambda pubblica una notifica Amazon SNS su quello esistente. `SO0111-ASR-MigrationAutoRemediation` `SO0111-ASR_Topic` Per ricevere tale notifica, devi avere un abbonamento confermato prima di iniziare l'aggiornamento dello stack v4. **`SO0111-ASR_Topic`** Fare riferimento a Aggiornamento da v2.x a v4.0.0 o versioni successive.
- Aggiornamento alla versione 3.x dalla versione 2.x: Re-enable regole di correzione automatica manualmente nell'account Admin dopo l'aggiornamento dello stack. Fai riferimento a Abilita correzioni completamente automatiche.
- Se utilizzi il `Reuse Orchestrator Log Group` parametro per conservare i log, assicurati che sia impostato correttamente durante l'aggiornamento dello stack per evitare la ricreazione dei gruppi di log o la perdita delle impostazioni di conservazione dei log. Fai riferimento a Implementare la soluzione. Se stai eseguendo un aggiornamento dello stack alla v2.3.0+ da una versione precedente, scegli «no»

Aggiornamento da versioni precedenti alla v1.4

Se hai già distribuito la soluzione prima della v1.4.x, disinstalla e installa la versione più recente:

1. Disinstalla la soluzione precedentemente distribuita. Fai riferimento a Disinstallare la soluzione.
2. Avvia il modello più recente. Fai riferimento a Distribuire la soluzione.

> **Note**
>
> Se stai effettuando l'aggiornamento dalla versione 1.2.1 o precedente alla versione 1.3.0 o successiva, imposta su. `Reuse Orchestrator Log Group` No Se stai reinstallando la versione 1.3.0 o successiva, puoi selezionare questa opzione. `Yes` Questa opzione consente di continuare ad accedere allo stesso gruppo di log per Orchestrator Step Functions.

Aggiornamento dalla versione 1.4 e successive

Se stai effettuando l'aggiornamento dalla v1.4.x, aggiorna tutti gli stack o come segue: StackSets

1. Aggiorna lo stack nell'account amministratore di Security Hub utilizzando il modello più recente. https://solutions-reference.s3.amazonaws.com/automated-security-response-on-aws/latest/automated-security-response-admin.template
2. In ogni account membro, aggiorna le autorizzazioni dal modello più recente.
3. In ogni account membro in tutte le regioni in cui è attualmente distribuito, aggiorna lo stack di membri dal modello più recente.
4. Se l'interfaccia utente Web è abilitata e hai aggiornato parametri come`TicketGenFunctionName`, ad esempio, invalida la CloudFront cache per riflettere immediatamente le modifiche:

```
aws cloudfront create-invalidation \
  --distribution-id <distribution-id> \
  --paths "/aws-exports.json"
```

Aggiornamento dalla versione 2.0.x

Se stai effettuando l'aggiornamento dalla v2.0.x, esegui prima l'aggiornamento alla v2.3.0. L'aggiornamento alla CloudFormation v2.1.0—2.1.1 non riesce.

L'aggiornamento dalla versione 2.1.4 o precedente

Se si esegue l'aggiornamento dalla v2.1.4 o precedente, è necessario eseguire l'aggiornamento alla v2.3.0 prima di eseguire l'aggiornamento a qualsiasi versione successiva alla v2.3.0. Altrimenti, l'operazione di aggiornamento dello stack fallirà. In alternativa, è possibile eliminare e ridistribuire gli stack della soluzione anziché eseguire un aggiornamento dello stack.

Aggiornamento da v2.x a v4.0.0 o successivo

A partire dalla versione 4.0.0, la soluzione mantiene le impostazioni di riparazione automatica durante l'aggiornamento dalla v2 alla v4. Nella versione 2, le regole Amazon per controllo memorizzavano lo stato di riparazione automatica. EventBridge Nella versione 3 e successive, la soluzione lo memorizza nella tabella Amazon DynamoDB di Remediation Configuration nell'account amministratore. Durante l'aggiornamento dello stack v4, una risorsa personalizzata analizza `_AutoTrigger` le regole v2 esistenti, traduce l'ID di controllo specifico di ciascuna regola nell'ID di controllo di sicurezza corrispondente e scrive i controlli precedentemente abilitati nella tabella DynamoDB.

La migrazione riguarda tutti e cinque i playbook v2:

- `SC`(controlli di sicurezza di AWS Service-managed Security Hub): gli ID di controllo vengono scritti in DynamoDB senza modifiche.
- `AFSBP`(AWS Foundational Security Best Practices): gli ID di controllo vengono scritti in DynamoDB senza modifiche.
- `NIST80053R5`(NIST 800-53 Revision 5): gli ID di controllo vengono scritti in DynamoDB senza modifiche.
- `PCI`(PCI DSS v3.2.1): il prefisso iniziale viene rimosso (ad esempio, diventa). `PCI. PCI.S3.5 S3.5`
- `CIS`(CIS AWS Foundations Benchmark v1.2.0, v1.4.0 e v3.0.0): ogni ID di controllo CIS è associato al controllo di sicurezza a cui è destinato il documento di correzione SSM v2 a cui è destinato.

Risultati della migrazione:

- I controlli migrati correttamente non richiedono alcuna azione: la correzione automatica è abilitata nella v4 nello stesso modo in cui lo erano nella v2.

- I controlli ignorati dalla migrazione si dividono in due categorie: le regole CIS senza una correzione ASR nella v2 e i controlli v3+ non vengono forniti. I controlli ignorati sono elencati nei log Amazon della funzione AWS Lambda. `SO0111-ASR-MigrationAutoRemediation` CloudWatch
- Se la migrazione rileva un errore per ogni controllo (ad esempio, un errore di limitazione transitorio durante l'aggiornamento di DynamoDB) o si interrompe prima che i controlli vengano scritti, pubblica una notifica Amazon SNS sull'argomento esistente. `SO0111-ASR-MigrationAutoRemediation` `SO0111-ASR_Topic` Il corpo della notifica elenca gli ID di controllo interessati ed è preceduto da. `[ASR v2 # v3/v4 migration]`
- La risorsa personalizzata viene eseguita solo durante l'aggiornamento iniziale v3/v4 dello stack. Gli aggiornamenti successivi dello stack non eseguono nuovamente la migrazione.

> **Note**
>
> Abbonati all'argomento SNS prima dell'aggiornamento. Le notifiche di errore di migrazione vengono pubblicate nell'argomento `SO0111-ASR_Topic` Amazon SNS esistente della soluzione. Se non disponi di un abbonamento confermato su quell'argomento prima dell'aggiornamento, la notifica di errore non ti arriva. In tal caso, l'errore viene visualizzato solo nei CloudWatch log Amazon della funzione `SO0111-ASR-MigrationAutoRemediation` AWS Lambda. Per sottoscrivere un endpoint, recupera l'argomento ARN da AWS Systems Manager Parameter Store all'indirizzo `/Solutions/SO0111/SNS_Topic_ARN` e aggiungi un abbonamento SNS (email, SQS, funzione AWS Lambda o qualsiasi altro protocollo supportato) prima di iniziare l'aggiornamento dello stack v4. Conferma eventuali sottoscrizioni e-mail tramite l'e-mail di conferma di AWS in modo che l'argomento sia pronto per la pubblicazione prima dell'esecuzione della migrazione.

Se la migrazione non è in grado di scrivere un controllo da correggere automaticamente nella v4, abilitalo manualmente nella tabella Remediation Configuration DynamoDB. Fai riferimento a Abilita correzioni completamente automatiche. ???

Risoluzione dei problemi

La risoluzione dei problemi noti fornisce istruzioni per mitigare gli errori noti. Se queste istruzioni non risolvono il problema, Contact AWS Support fornisce istruzioni per aprire un caso AWS Support per questa soluzione.

Log della soluzione

Questa sezione include informazioni sulla risoluzione dei problemi per questa soluzione, consulta la barra di navigazione a sinistra per gli argomenti.

Questa soluzione raccoglie l'output dai runbook di riparazione, eseguiti in AWS Systems Manager, e registra il risultato `SO0111-ASR` nel gruppo CloudWatch Logs nell'account amministratore di AWS Security Hub. C'è un flusso per controllo al giorno.

Orchestrator Step Functions registra tutte le transizioni di fase nel `SO0111-ASR-Orchestrator` CloudWatch Logs Group nell'account amministratore di AWS Security Hub. Questo registro è un audit trail per registrare le transizioni di stato per ogni istanza di Step Functions. Esiste un flusso di log per esecuzione di Step Functions.

Entrambi i gruppi di log sono crittografati utilizzando una chiave gestita dal cliente di AWS KMS.

Le seguenti informazioni sulla risoluzione dei problemi utilizzano il gruppo di `SO0111-ASR` log. Usa questo registro, insieme alla console di AWS Systems Manager Automation, ai log di Automation Executions, alla console Step Function e ai log Lambda per risolvere i problemi.

Se una soluzione non riesce, `SO0111-ASR` nel flusso di log verrà registrato un messaggio simile al seguente per lo standard, il controllo e la data. Ad esempio, CIS-2.9-2021-08-12

```
ERROR: a4cbb9bb-24cc-492b-a30f-1123b407a6253: Remediation failed for CIS control
 2.9 in account 123412341234: See Automation Execution output for details (AwsEc2Vpc
 vpc-0e92bbe911cf08acb)
```

I seguenti messaggi forniscono ulteriori dettagli. Questo risultato è tratto dal runbook ASR per lo standard e il controllo di sicurezza. Ad esempio: _1.2.0_2.9 ASR-CIS

```
Step fails when it is Execution complete: verified. Failed to run automation with
 executionId: eecdef79-9111-4532-921a-e098549f5259 Failed :
```

```
{Status=[Failed], Output=[No output available yet because the step is not successfully
 executed], ExecutionId=[eecdef79-9111-4532-921a-e098549f5259]}. Please refer to
 Automation Service Troubleshooting Guide for more diagnosis details.
```

Queste informazioni indicano l'errore, che in questo caso era un'automazione secondaria in esecuzione nell'account membro. Per risolvere questo problema, devi accedere alla Console di gestione AWS nell'account membro (dal messaggio precedente), accedere ad AWS Systems Manager, accedere ad Automation ed esaminare l'output del log per l'Execution ID. `eecdef79-9111-4532-921a-e098549f5259`

Risoluzione di problemi noti

- Problema: l'implementazione della soluzione non riesce con un errore che indica che le risorse sono già disponibili in Amazon. CloudWatch

  Risoluzione: verifica la presenza di un messaggio di errore nella CloudFormation resources/events sezione che indica che i gruppi di log esistono già. I modelli di distribuzione ASR consentono il riutilizzo dei gruppi di log esistenti. Verifica di aver selezionato il riutilizzo.

- Problema: la soluzione non viene implementata con un errore in uno stack annidato di un playbook in cui non viene creata una regola EventBridge

  Risoluzione: probabilmente hai raggiunto la quota di EventBridge regole con il numero di playbook implementati. Puoi evitarlo utilizzando i risultati di controllo consolidati in Security Hub abbinati al playbook SC di questa soluzione, implementando solo i playbook per gli standard utilizzati o richiedendo un aumento della quota delle regole. EventBridge

- Problema: eseguo Security Hub in più regioni con lo stesso account. Desidero implementare questa soluzione in più regioni.

  Risoluzione: implementa lo stack di amministrazione nello stesso account e nella stessa regione dell'amministratore di Security Hub. Installa il modello di membro in ogni account e regione in cui è configurato un membro del Security Hub. Abilita l'aggregazione nel Security Hub.

- Problema: subito dopo la distribuzione, SO0111-ASR-Orchestrator viene visualizzato un errore nel Get Automation Document State e viene visualizzato un errore 502: «`Lambda non è riuscita a decrittografare le variabili di ambiente perché l'accesso al KMS è stato negato. Controlla le impostazioni dei tasti KMS della funzione. Eccezione KMS: UnrecognizedClientExceptionKMS Messaggio: il token di sicurezza incluso nella richiesta non è valido. (Servizio: AWSlambda; Codice di stato: 502; Codice di errore:; ID richiesta: KMSAccessDeniedException... `»

Risoluzione: attendere che la soluzione si stabilizzi per circa 10 minuti prima di eseguire le riparazioni. Se il problema persiste, apri un ticket di assistenza o GitHub un problema.

- Problema: ho tentato di rimediare a un problema ma non è successo niente.

  Risoluzione: controlla le note del risultato per scoprire i motivi per cui non è stato corretto. Una causa comune è che il risultato non prevede una correzione automatica. Al momento non è possibile fornire un feedback diretto all'utente quando non esiste alcuna correzione se non tramite le note. Esamina i log della soluzione. Apri CloudWatch i log nella console. Trova il gruppo SO0111-ASR CloudWatch Logs. Ordina l'elenco in modo che gli stream aggiornati più di recente vengano visualizzati per primi. Seleziona il flusso di log per la ricerca che hai tentato di eseguire. Dovresti trovare eventuali errori lì. Alcuni motivi dell'errore potrebbero essere: mancata corrispondenza tra il controllo della ricerca e il controllo della correzione, la correzione tra più account (non ancora supportata) o il fatto che il risultato sia già stato corretto. Se non riesci a determinare il motivo dell'errore, raccogli i log e apri un ticket di assistenza.

- Problema: dopo aver avviato una correzione, lo stato nella console di Security Hub non è stato aggiornato.

  Risoluzione: la console Security Hub non si aggiorna automaticamente. Aggiorna la visualizzazione corrente. Lo stato del risultato dovrebbe essere aggiornato. Potrebbero essere necessarie diverse ore prima che il risultato passi da Non riuscito a superato. I risultati vengono creati dai dati degli eventi inviati da altri servizi, come AWS Config, ad AWS Security Hub. Il tempo necessario prima che una regola venga rivalutata dipende dal servizio sottostante. Se ciò non risolve il problema, fate riferimento alla risoluzione precedente per «`Ho tentato di rimediare a un risultato ma non è successo nulla. `»

- Problema: la funzione Orchestrator step non riesce in Get Automation Document State: si è verificato un errore (AccessDenied) durante la chiamata dell'operazione. AssumeRole

  Risoluzione: il modello di membro non è stato installato nell'account membro in cui ASR sta tentando di porre rimedio a un risultato. Segui le istruzioni per la distribuzione del modello di membro.

- Problema: il Config.1 runbook non funziona perché il registratore o il canale di consegna esistono già.

  Risoluzione: controlla attentamente le impostazioni di AWS Config per assicurarti che Config sia configurato correttamente. In alcuni casi, la correzione automatica non è in grado di correggere le impostazioni AWS Config esistenti.

- Problema: la riparazione ha esito positivo ma restituisce il messaggio `"No output available yet because the step is not successfully executed."`

  Risoluzione: si tratta di un problema noto in questa versione a causa del quale alcuni runbook di riparazione non restituiscono una risposta. I runbook di riparazione falliranno correttamente e segnaleranno la soluzione se non funzionano.

- Problema: la risoluzione non è riuscita e ha inviato una traccia dello stack.

  Risoluzione: di tanto in tanto, perdiamo l'opportunità di gestire una condizione di errore che si traduce in una traccia dello stack anziché in un messaggio di errore. Tentativo di risolvere il problema a partire dai dati di tracciamento. Apri un ticket di supporto se hai bisogno di assistenza.

- Problema: la rimozione dello stack v1.3.0 non è riuscita sulla risorsa Custom Action.

  Risoluzione: la rimozione del modello di amministrazione potrebbe non riuscire durante la rimozione di Custom Action. Si tratta di un problema noto che verrà risolto nella prossima versione. Se si verifica questo problema:

  a. Accedi alla console di gestione di AWS Security Hub.

  b. Nell'account amministratore, vai su Impostazioni.

  c. Seleziona la scheda Azioni personalizzate

  d. Eliminare manualmente la voce Remediate with ASR.

  e. Elimina nuovamente la pila.

- Problema: dopo aver ridistribuito lo stack di amministrazione, la funzione Step non funziona. `AssumeRole`

  Risoluzione: la ridistribuzione dello stack di amministrazione interrompe la connessione di fiducia tra il ruolo di amministratore nell'account amministratore e il ruolo di membro negli account membri. È necessario ridistribuire lo stack dei ruoli dei membri in tutti gli account membri.

- Problema: le correzioni CIS 3.x non vengono visualizzate `PASSED` dopo più di 24 ore.

  Risoluzione: si tratta di un evento comune se non hai sottoscrizioni all'argomento `SO0111-ASR_LocalAlarmNotification` SNS nell'account del membro.

Problemi relativi a soluzioni correttive specifiche

SetSSLBucketPolicy fallisce con un AccessDenied errore

Controlli associati: AWS FSBP v1.0.0 S3.5, PCI v3.2.1, CIS v1.4.0 2.1.2, SC PCI.S3.5 v2.0.0 S3.5

SetSSLBucketPolicy Problema: il file AccessDenied fallisce con un errore:

Si è verificato un errore (AccessDenied) durante la chiamata all' PutBucketPolicy operazione: Accesso negato

Se l'impostazione Blocca accesso pubblico è stata abilitata per un bucket, i tentativi di inserire una policy del bucket che include istruzioni che consentono l'accesso pubblico falliranno con questo errore. Questo stato può essere raggiunto inserendo una policy del bucket che contenga tali istruzioni, quindi abilitando il blocco di accesso pubblico per quel bucket.

La correzione ConfigureS3BucketPublicAccessBlock (controlli associati: AWS FSBP v1.0.0 S3.2, PCI v3.2.1, CIS v1.4.0 2.1.5.2 PCI.S3.2, SC v2.0.0 S3.2) può anche mettere un bucket in questo stato perché imposta l'impostazione del blocco di accesso pubblico senza modificare la politica del bucket.

SetSSLBucketPolicy Aggiunge una dichiarazione alla policy del bucket per rifiutare le richieste che non utilizzano SSL. Non modifica le altre dichiarazioni della policy, quindi se sono presenti istruzioni che consentono l'accesso pubblico, la correzione fallirà nel tentativo di inserire la policy del bucket modificata che include ancora tali istruzioni.

Risoluzione: modifica la policy del bucket per rimuovere le istruzioni che consentono l'accesso pubblico in conflitto con l'impostazione di blocco dell'accesso pubblico sul bucket.

PutS3BucketPolicyDeny fallisce

Controlli associati: AWS FSBP v1.0.0 S3.6, (1), NIST.800-53.r5 CA-9 NIST.800-53.r5 CM-2

Problema: PutS3BucketPolicyDeny con il seguente errore:

```
Unable to create an explicit deny statement for {bucket_name}.
```

Se i principi per tutte le politiche sul bucket di destinazione sono «*», la soluzione non può aggiungere la policy deny al bucket di destinazione poiché bloccherebbe tutte le azioni del bucket per tutti i principali.

Risoluzione: modifica la policy del bucket per consentire azioni su account specifici invece di utilizzare i principi «*» e limita le azioni negate.

Come disattivare la soluzione

In caso di incidente, è possibile che sia necessario disattivare la soluzione senza rimuovere alcuna infrastruttura. Questi scenari descrivono in dettaglio come disabilitare i diversi componenti della soluzione.

Scenario 1: disabilitare la riparazione automatica per un singolo controllo

1. Nell'account Admin, accedi alla CloudFormation console https://console.aws.amazon.com/cloudformation/home? AWS.
2. Individua lo stack di amministrazione e visualizza la relativa scheda Outputs.
3. Copia il valore dell'`RemediationConfigurationDynamoDBTable`output.
4. Accedi alla console DynamoDB e apri la tabella Remediation Configuration.
5. Seleziona Explore Table Items (Esplora elementi della tabella).
6. In Elementi di scansione o interrogazione, seleziona Query.
7. Inserisci l'ID di controllo (ad esempio,`Lambda.1`) nel campo Chiave di partizione: ControlID e scegli Esegui.
8. Seleziona l'elemento restituito, quindi scegli Azioni > Modifica elemento.
9. Cambia il valore dell'`automatedRemediationEnabled`attributo su False.
10. Scegliete Salva e chiudi.

Scenario 2: disabilita la riparazione automatica per tutti i controlli

1. Segui i passaggi 1-5 dello Scenario 1 per accedere agli elementi della tabella di configurazione della riparazione.
2. In Elementi di scansione o interrogazione, seleziona Scansione per visualizzare tutti i controlli.
3. Per ogni controllo `automatedRemediationEnabled` impostato su True, seleziona l'elemento e scegli Azioni > Modifica elemento.
4. Modificate il valore dell'`automatedRemediationEnabled`attributo su False e scegliete Salva e chiudi.
5. Ripeti l'operazione per tutti i controlli che desideri disattivare.

Scenario 3: disabilita la correzione manuale per un account

1. Passare alla console EventBridge .
2. Seleziona Regole nella barra laterale.
3. Seleziona il bus di eventi predefinito e cerca. `Remediate_with_ASR_CustomAction`
4. Seleziona la regola e scegli il pulsante Disabilita.

Contattare AWS Support

Se disponi di AWS Business Support+, AWS Enterprise Support o Unified Operations, puoi utilizzare AWS Support Center per ottenere assistenza da parte di esperti con questa soluzione. Le istruzioni per eseguire tali operazioni sono fornite nelle sezioni seguenti.

Crea un caso

1. Accedi al Centro assistenza.
2. Scegli Crea caso.

Come possiamo aiutarti?

1. Scegli Tecnico.
2. Per Assistenza, seleziona Soluzioni.
3. Per Categoria, seleziona Automated Security Response on AWS.
4. Per Severity, seleziona l'opzione più adatta al tuo caso d'uso.
5. Quando si inseriscono i campi Servizio, Categoria e Severità , l'interfaccia popola i collegamenti alle domande più comuni per la risoluzione dei problemi. Se non riesci a risolvere la tua domanda con questi link, scegli Passaggio successivo: Informazioni aggiuntive.

Informazioni aggiuntive

1. Per Oggetto, inserisci il testo che riassuma la domanda o il problema.
2. Per la descrizione, descrivi il problema in dettaglio, includendo il nome di questa soluzione e la versione che stai utilizzando, ad esempio: Automated Security Response on AWS v. X.Y.Z
3. Scegli Allega file.
4. Allega le informazioni necessarie all'assistenza per elaborare la richiesta.

Aiutaci a risolvere il tuo caso più velocemente

1. Inserisci le informazioni richieste.
2. Scegli Passaggio successivo: risolvi ora o contattaci.

Risolvi ora o contattaci

1. Esamina le soluzioni Solve now.
2. Se non riesci a risolvere il problema con queste soluzioni, scegli Contattaci, inserisci le informazioni richieste e scegli Invia.

Disinstalla la soluzione

Utilizza la seguente procedura per disinstallare la soluzione con la Console di gestione AWS.

V1.0.0-V1.2.1

Per le versioni da v1.0.0 a v1.2.1, utilizza Service Catalog per disinstallare i playbook CIS, i playbook FSBP o entrambi. Con la versione 1.3.0, Service Catalog non viene più utilizzato.

1. Accedi alla CloudFormation console AWS e vai all'account principale di Security Hub.
2. Scegli Service Catalog per terminare qualsiasi playbook a cui è stato assegnato il provisioning, rimuovere gruppi, ruoli o utenti di sicurezza.
3. Rimuovi il `CISPermissions.template` modello di spoke dagli account dei membri del Security Hub.
4. Rimuovi il `AFSBPMemberStack.template` modello di spoke dagli account di amministrazione e dei membri di Security Hub.
5. Accedi all'account principale di Security Hub, seleziona lo stack di installazione della soluzione, quindi scegli Elimina.

> **Note**
>
> CloudWatch Log, i log di gruppo vengono conservati. Consigliamo di conservare questi registri come richiesto dalla politica di conservazione dei registri dell'organizzazione.

V1.3.x

1. Rimuovili `automated-security-response-member.template` da ogni account membro.
2. Rimuovi il file `automated-security-response-admin.template` dall'account amministratore.

> **Note**
>
> La rimozione del modello di amministrazione nella v1.3.0 probabilmente fallirà con la rimozione dell'azione personalizzata. Si tratta di un problema noto che verrà risolto nella prossima versione. Usa le seguenti istruzioni per risolvere il problema:
>
> 1. Accedi alla console di gestione di AWS Security Hub.
> 2. Nell'account amministratore, vai su Impostazioni.
> 3. Scegli la scheda Azioni personalizzate.
> 4. Eliminare manualmente la voce Remediate with ASR.
> 5. Elimina nuovamente la pila.

V1.4.0 e più tardi

Implementazione dello stack

1. Rimuovili `automated-security-response-member.template` da ogni account membro.
2. Rimuovi il file `automated-security-response-admin.template` dall'account amministratore.

StackSet distribuzione

Per ciascuno StackSet, rimuovi gli stack, quindi rimuovi StackSet nell'ordine inverso rispetto alla distribuzione.

Nota che i ruoli IAM di `automated-security-response-member-roles.template` vengono mantenuti anche se il modello viene rimosso. In questo modo le correzioni che utilizzano questi ruoli continuano a funzionare. Questi ruoli SO0111-* possono essere rimossi manualmente dopo aver verificato che non siano più utilizzati mediante correzioni attive, ad esempio CloudTrail alla CloudWatch registrazione, o RDS Enhanced Monitoring.

> **Note**
>
> Le tabelle Amazon DynamoDB della soluzione vengono conservate quando rimuovi lo stack di amministrazione, in modo da preservare la cronologia e la configurazione delle correzioni. Queste tabelle sono le tabelle Risultati, Cronologia delle riparazioni, Configurazione delle

riparazioni, Filtri delle risorse, Configurazione delle notifiche e Batches di notifica. Ognuna di esse ha la protezione dall'eliminazione abilitata. Per rimuovere una tabella, disabilita prima la relativa protezione dall'eliminazione, quindi elimina la tabella.
Anche tutti i segreti di AWS Secrets Manager che hai creato per Slack, JIRA o per ServiceNow i canali vengono conservati. Eliminali manualmente se non ti servono più.

Guida per l'amministratore

Abilitazione e disabilitazione di parti della soluzione

In qualità di amministratore della soluzione, hai i seguenti controlli sulle funzionalità della soluzione abilitate.

Dove vengono distribuiti gli stack dei membri e dei ruoli dei membri:

- Lo stack di amministrazione sarà in grado di avviare le correzioni (tramite azioni personalizzate o completamente automatizzate) solo negli account in cui gli stack di ruoli di membro e membro sono stati distribuiti con il numero di account amministratore fornito come valore di parametro.
- Per esonerare completamente gli account o le regioni dal controllo della soluzione, non distribuire gli stack di membri o ruoli di membro in tali account o regioni.

Configurazione dell'aggregazione per la ricerca di account e regioni in Security Hub:

- Lo stack di amministrazione sarà in grado di avviare le correzioni (tramite azioni personalizzate o completamente automatizzate) solo per i risultati che arrivano nell'account amministratore e nella regione.
- Per esonerare completamente gli account o le regioni dal controllo della soluzione, non includete tali account o regioni per inviare i risultati allo stesso account amministratore e alla stessa regione in cui è distribuito lo stack di amministrazione.

Quali stack annidati standard vengono distribuiti:

- Lo stack di amministrazione sarà in grado di avviare le correzioni (tramite azioni personalizzate o completamente automatizzate) solo per i controlli il cui runbook di controllo è distribuito nell'account e nella regione del membro di destinazione. Questi vengono implementati dallo stack dei membri per ogni standard.
- Lo stack di amministrazione può avviare correzioni completamente automatiche solo per i controlli abilitati nella tabella Amazon DynamoDB di Remediation Configuration. Questa tabella viene distribuita nell'account amministratore.
- Per semplicità, implementa gli standard in modo coerente tra i tuoi account amministratore e membro. Se ti interessano AWS FSBP e CIS v1.2.0, distribuisci questi due stack di

amministrazione annidati nell'account amministratore e distribuisci questi due stack di membri nidificati in ogni account membro e regione.

Quali runbook di controllo sono distribuiti in ogni stack di membri annidati:

- Lo stack di amministrazione sarà in grado di avviare le correzioni (tramite azioni personalizzate o completamente automatizzate) solo per i controlli il cui runbook di controllo è distribuito nell'account del membro di destinazione e nella regione dallo stack del membro per ogni standard.
- Per esercitare un controllo più preciso sui controlli abilitati per un particolare standard, ogni stack annidato per uno standard dispone di parametri per i quali vengono distribuiti i runbook di controllo. Imposta il parametro per un controllo sul valore «NOT Available» per annullare la distribuzione di quel runbook di controllo.

Parametri SSM per abilitare e disabilitare gli standard:

- Lo stack di amministrazione sarà in grado di avviare le correzioni (tramite azioni personalizzate o completamente automatizzate) solo per gli standard abilitati tramite il parametro SSM distribuito dallo stack di amministrazione standard.
- Per disabilitare uno standard, imposta il valore del parametro SSM con il percorso «//Solutions/SO0111<standard_name>/<standard_version>/status" su «No».

Per quali controlli è abilitata la correzione completamente automatica:

La soluzione offre due modi per abilitare o disabilitare la correzione completamente automatica. Entrambi scrivono nella stessa tabella Amazon DynamoDB di Remediation Configuration nell'account amministratore, in modo da rimanere sincronizzati.

- Interfaccia utente Web (consigliata se implementata). Gestisci la correzione completamente automatica dalla pagina Controlli. Gli amministratori e gli amministratori delegati possono abilitare o disabilitare la correzione automatica per controllo e applicare filtri di risorse riutilizzabili in base all'ambito in base ai quali si interviene sui risultati. Per disattivare la correzione automatica per tutti i controlli contemporaneamente, ad esempio durante un incidente, scegli Disabilita tutte le riparazioni automatiche. Questo pulsante non è disponibile per gli operatori dell'account (sola lettura) e quando la correzione automatica è già disattivata per tutti i controlli. Per informazioni dettagliate, consulta Gestire la correzione automatica.

- Configurazione precedente (nessuna interfaccia utente Web). Se non hai implementato l'interfaccia utente Web, abilita o disabilita la correzione completamente automatica modificando direttamente gli elementi nella tabella Remediation Configuration DynamoDB e stabilisci quali risultati vengono corretti con i parametri del filtro AWS Systems Manager. Per i passaggi, consulta Abilitare le correzioni completamente automatizzate. ??? Per disattivare rapidamente la riparazione automatica durante un incidente senza l'interfaccia utente Web, consulta gli scenari di disabilitazione in Risoluzione dei problemi. ???

Accesso all'interfaccia utente Web della soluzione:

- Quando viene implementato lo stack di amministrazione, si riceve un'e-mail con le credenziali temporanee per accedere all'interfaccia utente Web utilizzando l'indirizzo e-mail fornito durante la distribuzione.
- Utilizzando la pagina Invita utenti, gli amministratori e gli amministratori delegati possono invitare altri utenti ad accedere all'interfaccia utente Web e delegare l'accesso alla soluzione.
- Utilizzando la pagina Visualizza utenti, gli amministratori e gli amministratori delegati possono visualizzare e gestire gli utenti esistenti.
- Per ulteriori informazioni sulle autorizzazioni e su come utilizzare l'interfaccia utente Web della soluzione, consulta il. the section called “Interfaccia utente Web”

Esempi di notifiche SNS

Quando viene avviata una riparazione


```
{
 "severity": "INFO",
 "message": "00000000-0000-0000-0000-000000000000: Remediation queued for SC control
 RDS.13 in account 111111111111",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
```

```
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

Quando una riparazione ha esito positivo

```
{
 "severity": "INFO",
 "message": "00000000-0000-0000-0000-000000000000: Remediation succeeded for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

Quando una riparazione fallisce

```
{
 "severity": "ERROR",
 "message": "00000000-0000-0000-0000-000000000000: Remediation failed for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
```

```
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

Per configurare le notifiche

Oltre agli argomenti di Amazon SNS gestiti dalla soluzione descritti in Esempi di notifiche SNS, puoi creare configurazioni di notifica dall'interfaccia utente Web. Ogni configurazione controlla quali eventi vengono recapitati, dove vengono recapitati e cosa contiene ogni messaggio. La soluzione archivia le configurazioni nell'account amministratore e le applica ai risultati e alle correzioni aggregati a quell'account e alla regione.

> **Interfaccia utente Web richiesta**
>
> È possibile creare e gestire le configurazioni di notifica dall'interfaccia utente Web. È necessario abilitare l'interfaccia utente Web (distribuire i componenti dell'interfaccia utente Web all'avvio o all'aggiornamento dello stack di amministrazione) per creare e gestire le configurazioni delle notifiche.

Canali di notifica

Ogni configurazione di notifica fornisce eventi attraverso uno o più canali. La soluzione supporta i seguenti tipi di canali:

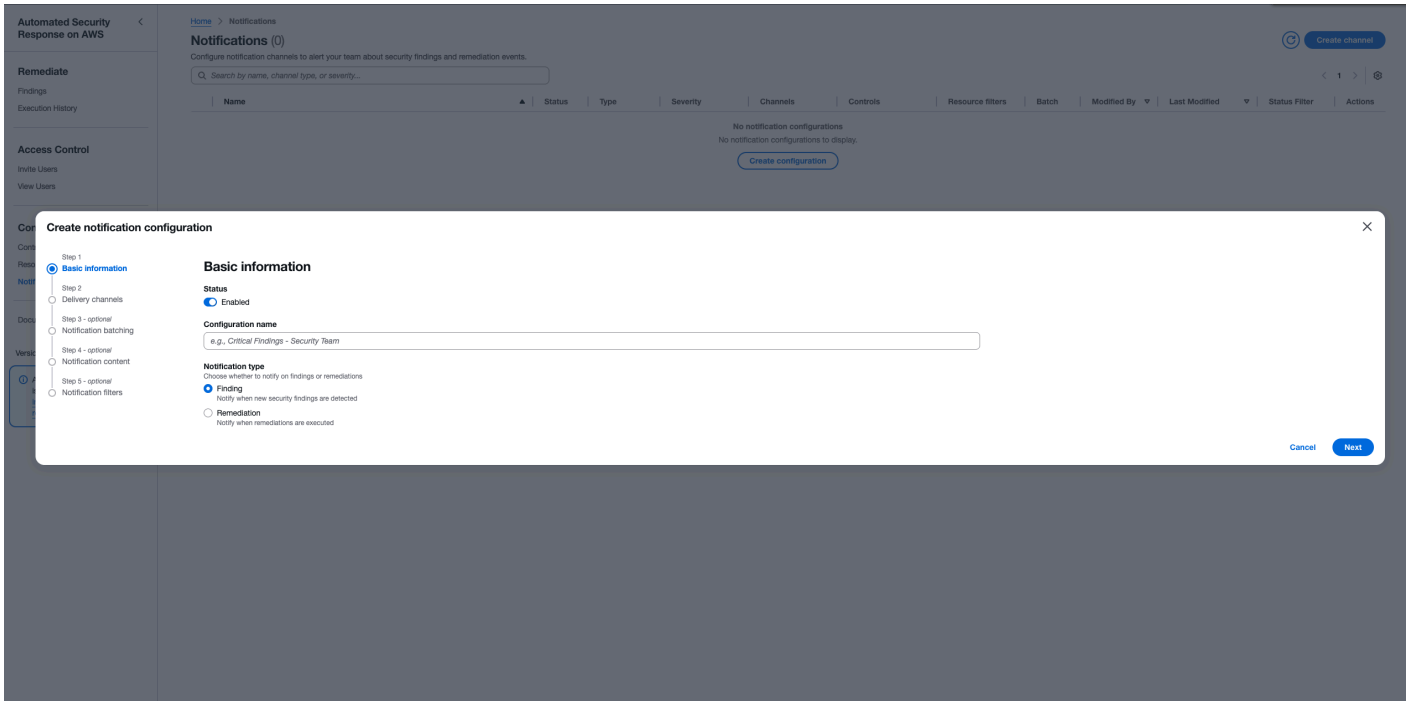
Canale	Description
Email	Invia e-mail ai destinatari selezionati. I destinatari possono essere scelti in base al ruolo (contatto principale dell'account, contatto di sicurezza, contatto operativo, operatori dell'account) o inseriti come indirizzi e-mail personalizzati. I destinatari delle e-mail personalizzate devono confermar e l'iscrizione prima di ricevere messaggi.
Slack	Pubblica messaggi su un canale Slack. Richiede l'ID del canale Slack e un segreto di AWS Secrets Manager contenente le credenziali Slack.

Canale	Description
JIRA	Crea un problema JIRA. Richiede l'URL dell'istanza JIRA, la chiave del progetto, il tipo di problema e un segreto di Secrets Manager contenente le credenziali JIRA.
ServiceNow	Crea un record in una tabella. ServiceNow Richiede l'URL dell' ServiceNow istanza, il nome della tabella e un segreto di Secrets Manager contenente la chiave ServiceNow API.
Amazon SNS	Pubblica su un argomento Amazon SNS nell'account amministratore e nella regione.

> **Important**
>
> La soluzione legge le credenziali per Slack, JIRA e i ServiceNow canali da AWS Secrets Manager. Il nome segreto deve iniziare con `asr/notifications/` (ad esempio,). `arn:aws:secretsmanager:us-east-1:111111111111:secret:asr/notifications/servicenow-creds` L'URL dell'istanza per JIRA e ServiceNow i canali deve utilizzare HTTPS.

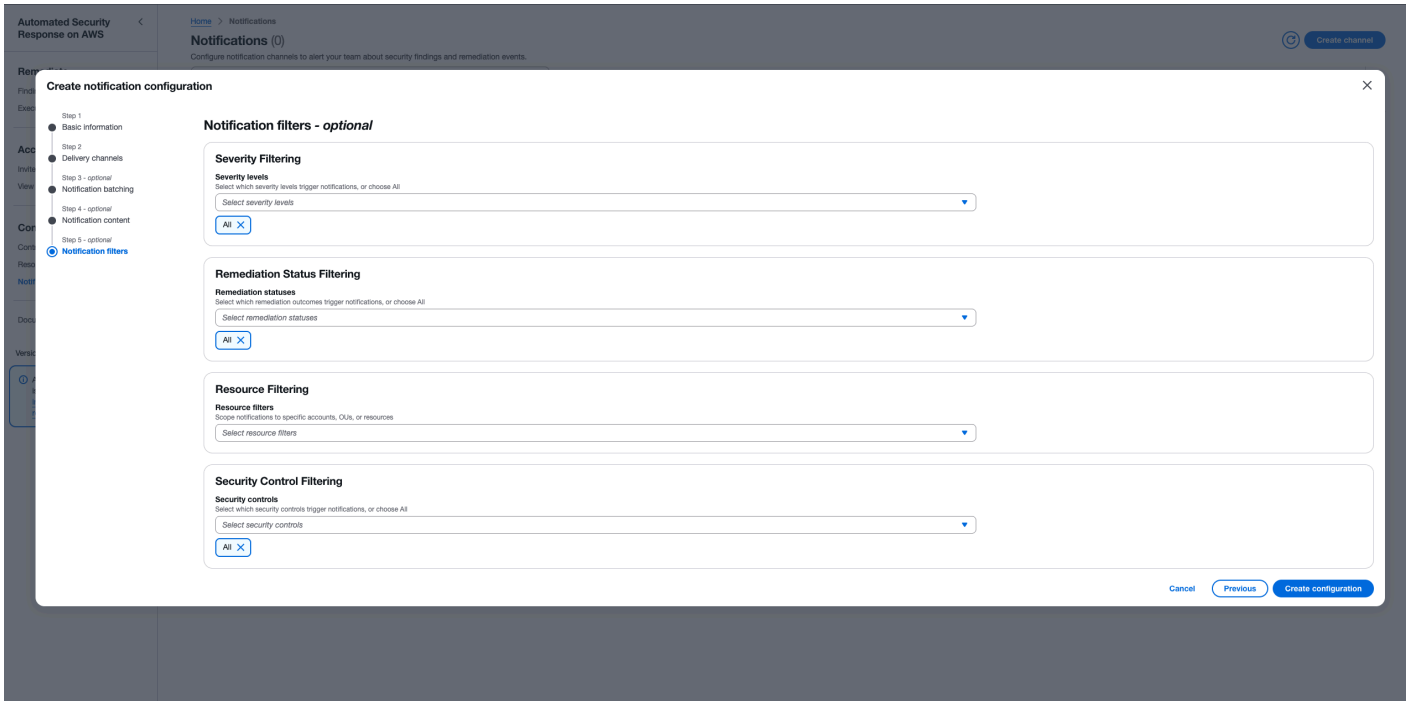
Crea una configurazione di notifica

1. Apri l'interfaccia utente Web e vai alla pagina Notifiche.
2. Scegli Crea configurazione delle notifiche.

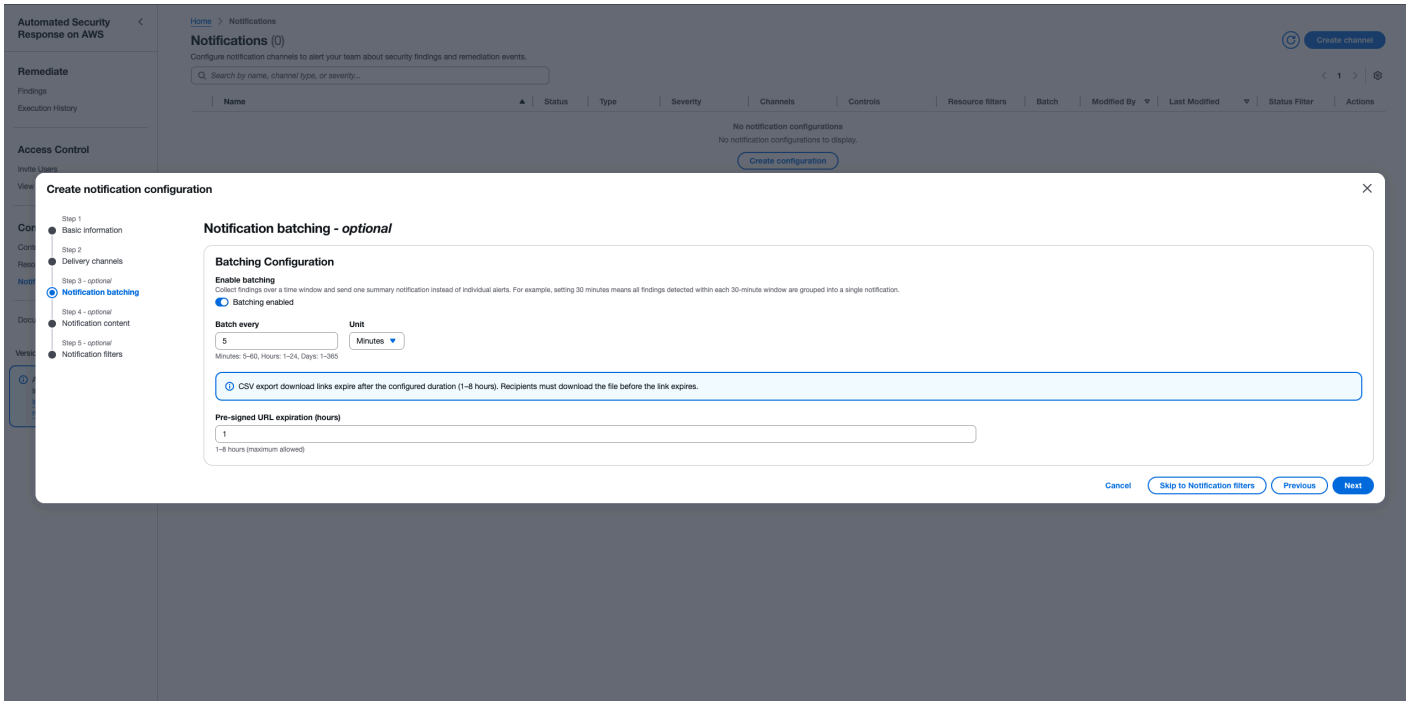


3. Informazioni di base: inserisci un nome di configurazione e scegli il tipo di notifica:
   a. Ricerca: invia una notifica quando vengono rilevati nuovi risultati.
   b. Correzione: notifica quando vengono eseguite le correzioni.
4. Canali di distribuzione: seleziona uno o più canali e fornisci la loro configurazione. È necessario abilitare almeno un canale.

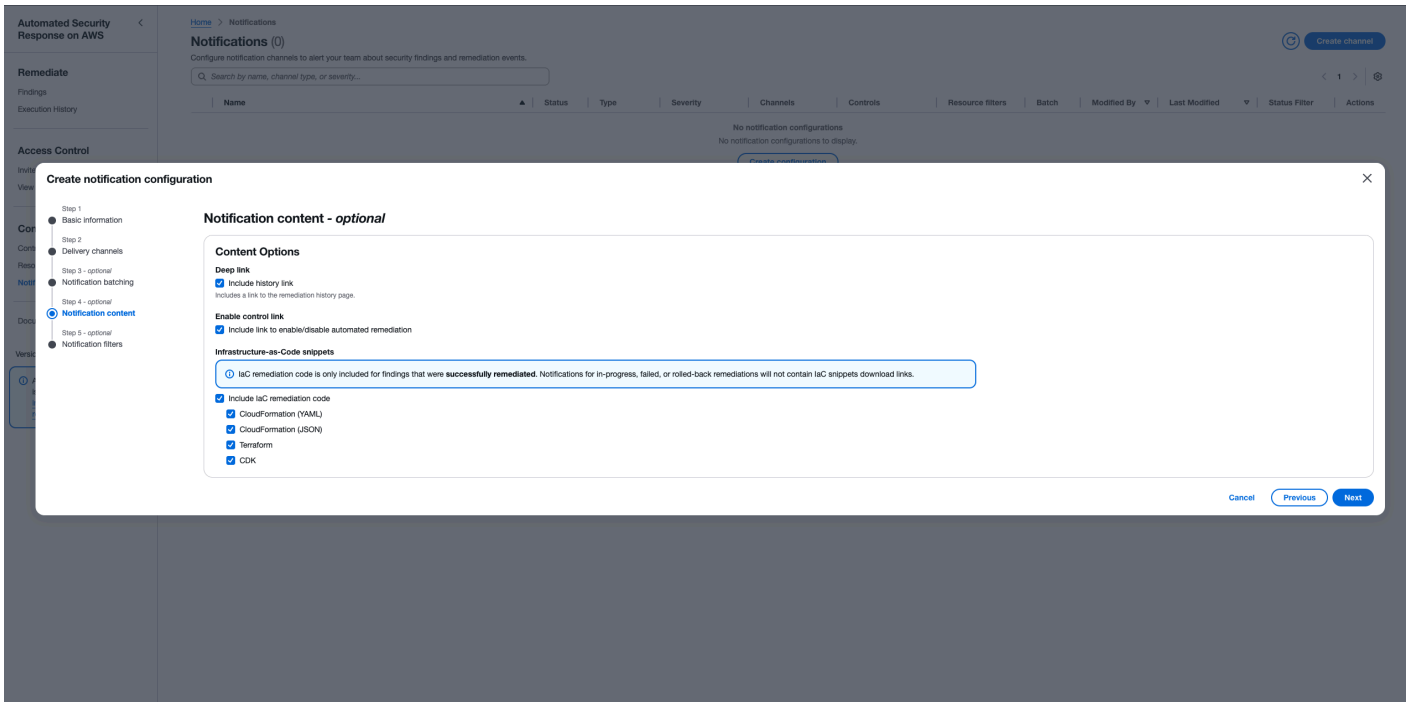
5. Filtri (Facoltativo): restringi gli eventi corrispondenti alla configurazione in base alla gravità, allo stato della correzione (solo tipo di riparazione), agli ID di controllo o ai filtri delle risorse. Se si lascia un filtro impostato su Tutti, non viene applicata alcuna restrizione a tale dimensione.



6. (Facoltativo) Batching: abilita una finestra batch per raggruppare più eventi in un'unica notifica. La durata della finestra batch deve rientrare nei seguenti intervalli: 5—60 minuti, 1—24 ore, 1—365 giorni.



7. Opzioni di contenuto: scegli cosa include ogni messaggio. Vedi Opzioni relative ai contenuti delle notifiche.



8. Seleziona Invia.

Opzioni relative ai contenuti delle notifiche

Le opzioni di contenuto controllano cosa include ogni messaggio di notifica. Le seguenti opzioni aggiungono ciascuna un link o uno snippet al messaggio:

Opzione	Description
`includeManualRemediationLink`	Aggiunge un link alla pagina dei risultati nell'interfaccia utente Web, in cui un operatore può eseguire la correzione manualmente.
`includeEnableAutomationLink`	Aggiunge un collegamento alla pagina dell'interfaccia utente Web per abilitare la correzione completamente automatica del controllo.

Opzione	Description
`includeIaCSnippet`	Aggiunge uno snippet di infrastructure-as-code per la correzione nei formati selezionati (YAML, JSON, Terraform o CDK). CloudFormation CloudFormation Si applica alle notifiche di tipo correttivo.
`includeRemediationDeadline`	Aggiunge una data di scadenza per ogni notifica per un risultato corrispondente. Si applica alle notifiche di tipo finding. Se abilitato, imposta `remediationDeadlineDays` (1—90). Vedi Scadenze per le riparazioni e applicazione delle scadenze.

> **I collegamenti richiedono l'interfaccia utente Web**
>
> Le `includeEnableAutomationLink` opzioni `includeManualRemediationLink` and aggiungono collegamenti alle pagine dell'interfaccia utente Web. L'interfaccia utente Web deve essere abilitata per la risoluzione di questi collegamenti. Se l'interfaccia utente Web non è distribuita, non abilitare queste opzioni.

Scadenze per la riparazione e applicazione delle scadenze

Una configurazione di notifica di tipo finding può assegnare una scadenza per la correzione a ogni risultato a cui corrisponde e, facoltativamente, far rispettare tale scadenza correggendo automaticamente le risultanze scadute.

Scadenze per le riparazioni

Abilita l'opzione di `includeRemediationDeadline` contenuto su una configurazione del tipo di ricerca e imposta un valore compreso tra `remediationDeadlineDays` 1 e 90. Per ogni risultato che corrisponde alla configurazione, la soluzione calcola una data di scadenza (l'ora di creazione della ricerca più il numero di giorni configurato) e la include nella notifica.

Di per sé, le scadenze sono informative. La data di scadenza viene visualizzata nella notifica, ma una volta trascorsa non accade nulla: la soluzione non interviene in caso di accertamento scaduto a meno che non si abiliti anche l'applicazione.

Applicazione delle scadenze

> **Warning**
>
> Quando abiliti l'`enforceDeadline`opzione su una configurazione di tipo finding, le scadenze per le correzioni smettono di essere indicative e diventano esecutive. La soluzione attiva automaticamente l'Orchestrator per porre rimedio a qualsiasi risultato irrisolto e scaduto che corrisponde alla configurazione, senza alcun intervento umano. Ciò vale indipendentemente dal fatto che il controllo del risultato abbia abilitato o meno la correzione automatica. Attivate l'applicazione solo per le configurazioni per le quali ritenete che la soluzione risolva automaticamente i risultati corrispondenti.

> **Periodo di tolleranza minimo di 24 ore**
>
> La soluzione non porrà mai rimedio a una constatazione avvenuta meno di 24 ore dopo la sua entrata in vigore, nemmeno per un arretrato preesistente la cui scadenza per la creazione è già scaduta. Questa soglia minima di 24 ore è fissa e non configurabile ed è separata (e aggiuntiva) dall'intervallo da 1 a 90 giorni. `remediationDeadlineDays`
> Di conseguenza, l'attivazione dell'applicazione di un backlog esistente non attiva una correzione di massa nel momento in cui viene attivata. Ogni risultato corrispondente riceve almeno 24 ore di preavviso prima che la soluzione possa porvi rimedio.

Prerequisiti e ambito

- Finding-type solo. L'applicazione è supportata solo nelle configurazioni di notifica di tipo finding, non nelle configurazioni di tipo remediation.
- Scadenza obbligatoria. La configurazione deve essere `includeRemediationDeadline` abilitata e `remediationDeadlineDays` impostata su un valore compreso tra 1 e 90.
- Interfaccia utente Web richiesta. Le configurazioni di notifica vengono create e gestite dall'interfaccia utente Web, pertanto è necessario implementare l'interfaccia utente Web.
- Config-boundary ambito. L'applicazione si applica ai risultati che corrispondono ai filtri di controllo, gravità e risorse della configurazione: il limite notification-config, non il limite di controllo. Non dipende dal fatto che il controllo corrispondente abbia abilitato la correzione automatica. In pratica, solo le risultanze che non sono già state corrette automaticamente entrano in vigore.

ServiceNow mappature personalizzate dei campi

Le mappature personalizzate dei campi consentono di aggiungere coppie chiave-valore al record creato per un risultato. ServiceNow Il valore può includere variabili modello che la soluzione sostituisce dal risultato al momento dell'invio. La chiave è il nome della ServiceNow colonna nella tabella di destinazione.

Le seguenti variabili di modello sono supportate nel valore:

- `${FINDING_ID}`
- `${CONTROL_ID}`
- `${SEVERITY}`
- `${ACCOUNT_ID}`
- `${REGION}`
- `${RESOURCE_ARN}`
- `${CONFIG_NAME}`

La soluzione impone i seguenti vincoli sulle mappature dei campi personalizzate:

- Fino a 20 mappature per canale.
- Lunghezza della chiave fino a 64 caratteri; lunghezza del valore risolto fino a 256 caratteri.
- Non utilizzare i seguenti campi gestiti dalla soluzione come chiavi:`short_description`,,, `descriptionurgency`,`impact`. `work_notes`

> **Important**
>
> La soluzione scrive i dati di ricerca ServiceNow così come sono e non esegue HTML-encode né sanifica i valori inviati. Associa i campi personalizzati solo ai campi di dati standard (ad esempio, campi String semplici). Non mapparli a:
>
> - campi HTML o campi journal/journal -input, che possono rendere HTML, oppure
> - Campi script (`script`,`script_plain`), che possono essere valutati tramite codice lato server.

Un semplice campo String visualizza i valori come testo. I campi HTML e journal possono eseguire il rendering del markup. La ricerca di dati, ad esempio un identificatore di risorsa, potrebbe contenere caratteri che l' ServiceNow istanza rende come markup. Il rendering o l'escape dei valori memorizzati dipendono dalle impostazioni di protezione avanzate dell' ServiceNow istanza (ad esempio, HTML escape e HTML sanitizer), che possiedi e che dovresti mantenere abilitate. Preferisci le colonne personalizzate definite dal cliente (in genere con prefisso u_ ox_) rispetto ai campi predefiniti e conferma il tipo di campo di destinazione prima della mappatura.

Per ulteriori informazioni sul rafforzamento della ServiceNow sicurezza, consulta le seguenti risorse:

- ServiceNow convalida dell'input (rafforzamento della sicurezza dell'istanza)
- Visualizza le voci dei campi del diario in formato HTML (comportamento di escape predefinito ad alta sicurezza)

Gestisci la correzione automatica

Quando l'interfaccia utente Web è abilitata, gestisci la correzione automatica dalla pagina Controlli invece di modificare direttamente la tabella Amazon DynamoDB di Remediation Configuration o i parametri di AWS Systems Manager. Da questa pagina è possibile abilitare la correzione automatica per i singoli controlli e l'ambito su cui la soluzione interviene applicando filtri di risorse riutilizzabili.

Interfaccia utente Web obbligatoria

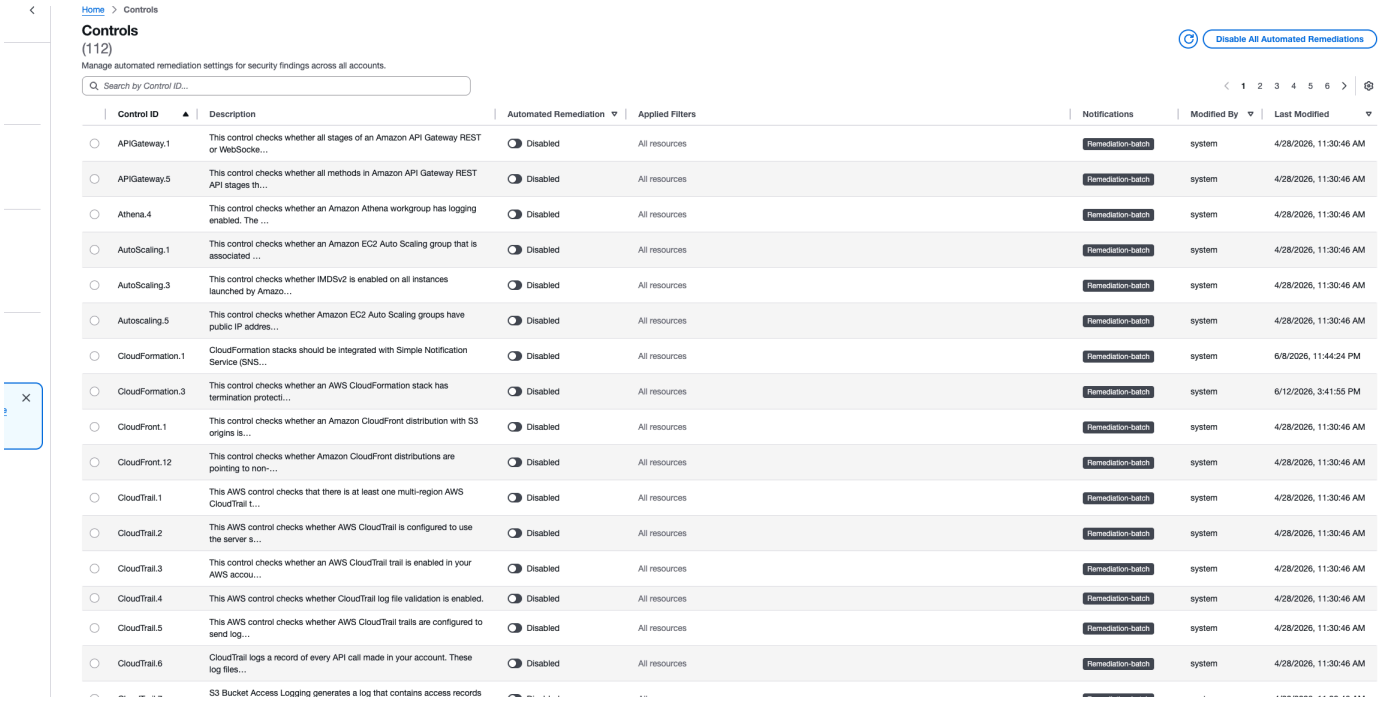
La pagina Controlli e i filtri delle risorse richiedono l'interfaccia utente Web. Se non hai implementato l'interfaccia utente Web, configura la correzione automatica tramite la tabella Remediation Configuration DynamoDB e i parametri del filtro di Systems Manager, come descritto in Abilita correzioni completamente automatiche. ???

L'accesso alla pagina Controlli segue gli stessi ruoli del resto dell'interfaccia utente Web. Gli amministratori e gli amministratori delegati possono abilitare o disabilitare la correzione automatica e creare, modificare e applicare filtri. Gli operatori degli account hanno accesso in sola lettura alle pagine Controlli e Filtri.

Abilita la correzione automatica per un controllo

La pagina Controlli elenca tutti i controlli di sicurezza supportati dalla soluzione, con lo stato attuale della correzione automatica, la descrizione e i filtri applicati. È possibile cercare e ordinare la tabella per ID di controllo o nome del filtro.

1. Apri l'interfaccia utente Web e vai alla pagina Controlli.



2. Imposta lo stato di riparazione automatica per uno o più controlli.
3. (Facoltativo) Applica uno o più filtri di risorse a un controllo e scegli una modalità di filtro (includi o escludi).
4. Scegli Salva per rendere permanenti le modifiche. La soluzione convalida e applica tutte le modifiche in sospeso insieme.

> **L'applicazione delle scadenze è un percorso separato verso la correzione automatica**
>
> L'attivazione della correzione automatica in questa pagina è il percorso principale: quando arriva un risultato corrispondente, la soluzione risolve il problema solo se il controllo è abilitato qui (soggetto a eventuali filtri di risorse applicati). Esiste un secondo percorso indipendente: l'applicazione delle scadenze. Se è `enforceDeadline` attiva una configurazione di notifica basata sul tipo di ricerca, la soluzione corregge automaticamente la corrispondenza dei risultati scaduti indipendentemente dal fatto che il controllo sia abilitato in questa pagina.

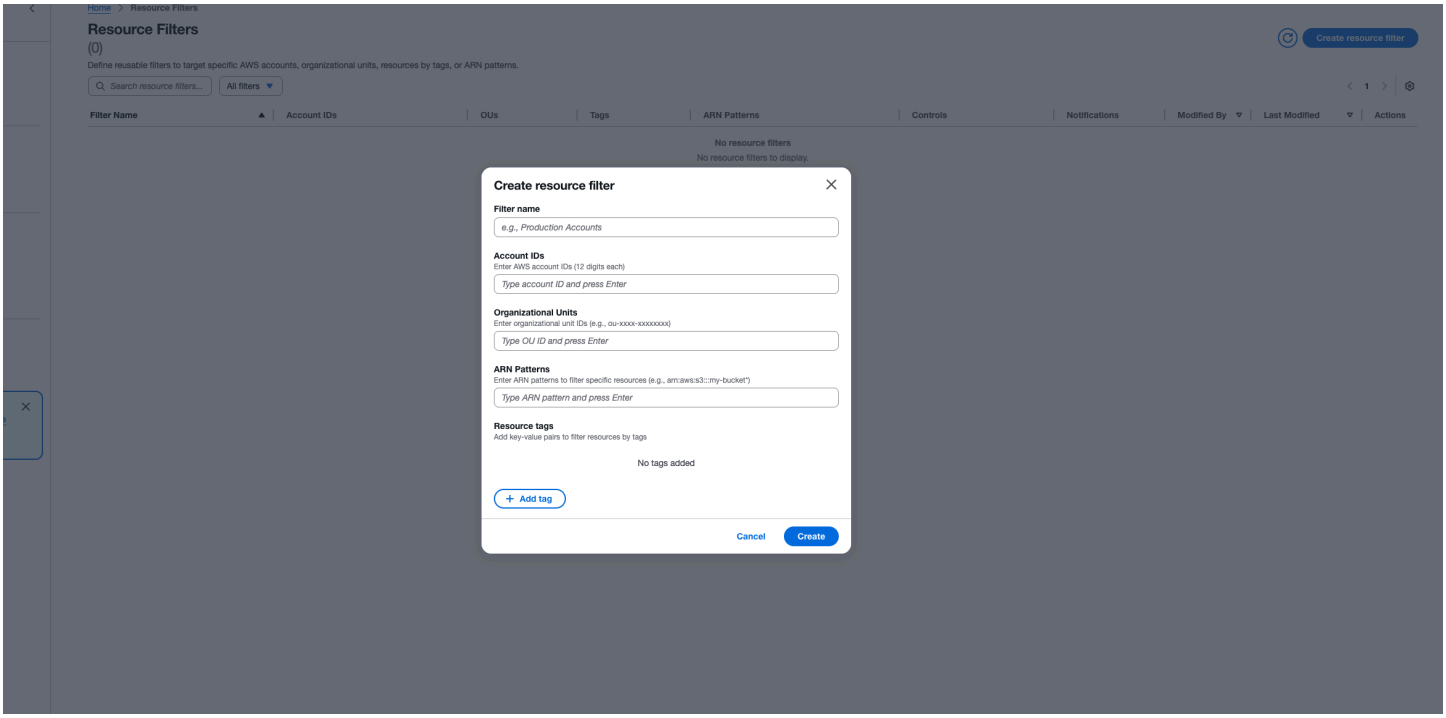
Se disabiliti un controllo qui per impedire la correzione automatica, conferma anche che nessuna configurazione di notifica applicata corrisponde a tali risultati. Per i dettagli, consulta Applicazione delle scadenze.

Crea e applica filtri per le risorse

Un filtro delle risorse è una definizione riutilizzabile che individua i risultati risolti automaticamente dalla soluzione. Ogni filtro può combinare i seguenti criteri:

- ID account: uno o più ID account AWS a 12 cifre.
- Unità organizzative: uno o più identificatori dell'unità organizzativa di AWS Organizations.
- Schemi ARN: uno o più modelli ARN di risorse. I pattern supportano il carattere jolly in qualsiasi componente ARN (ad esempio, `arn:aws:` corrisponde a qualsiasi risorsa nell'account). `111111111111`
- Tag di risorsa: una o più coppie chiave-valore di tag. La soluzione ignora i criteri di tag per i tipi di risorse che non possono essere etichettati, come gli utenti IAM e gli account AWS.

Per creare un filtro, apri la pagina Filtri e scegli Crea filtro, quindi inserisci un nome univoco e i criteri da abbinare.



Puoi applicare un filtro a un singolo controllo dalla pagina Controlli o a tutti i controlli contemporaneamente con l'azione Applica a tutti i controlli nella pagina Filtri. La rimozione di un filtro funziona allo stesso modo. L'eliminazione di un filtro lo rimuove da tutti i controlli che vi fanno riferimento.

Come vengono valutati i filtri

Quando arriva un risultato, il preprocessore decide se correggerlo automaticamente in base allo stato del controllo e ai filtri applicati a quel controllo:

- Se la correzione automatica è disattivata per il controllo, la soluzione non corregge il risultato.
- Se la correzione automatica è abilitata e il controllo non dispone di filtri, la soluzione corregge il risultato.
- Modalità Includi: la soluzione corregge il risultato solo quando corrisponde a tutti i filtri applicati al controllo (AND logico).
- Modalità di esclusione: la soluzione non corregge il risultato quando corrisponde a un filtro applicato al controllo.

Un risultato corrisponde a un filtro quando l'ID account, l'unità organizzativa, l'ARN della risorsa o i tag delle risorse del risultato corrispondono ai criteri corrispondenti nel filtro.

Tutorial

Questo è un tutorial che ti guiderà nella tua prima implementazione di ASR. Inizierà con i prerequisiti per l'implementazione della soluzione e terminerà con la correzione degli esempi riscontrati in un account membro.

Tutorial: Guida introduttiva alla risposta automatica alla sicurezza su AWS

Questo è un tutorial che ti guiderà nella prima implementazione. Inizierà con i prerequisiti per l'implementazione della soluzione e terminerà con la correzione degli esempi riscontrati in un account membro.

Prepara gli account

Per dimostrare le funzionalità di correzione della soluzione su più account e più regioni, questo tutorial utilizzerà due account. Puoi anche distribuire la soluzione su un singolo account.

Gli esempi seguenti utilizzano gli account `111111111111` e `222222222222` illustrano la soluzione. `111111111111`sarà l'account amministratore e `222222222222` sarà l'account membro. Prepareremo la soluzione per risolvere i problemi relativi alle risorse nelle Regioni `us-east-1` e `us-west-2`.

La tabella seguente è un esempio per illustrare le azioni che intraprenderemo per ogni fase in ogni account e regione.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
`111111111111`	Admin	Nessuno	Nessuno
`222222222222`	Membro	Nessuno	Nessuno

L'account amministratore è l'account che eseguirà le azioni di amministrazione della soluzione, vale a dire avviare le correzioni manualmente o abilitare le correzioni completamente automatiche utilizzando la tabella Remediation Configuration DynamoDB. Questo account deve anche essere

l'account amministratore delegato di Security Hub per tutti gli account in cui desideri correggere i risultati, ma non deve essere né deve essere l'account amministratore di AWS Organizations per l'AWS Organization a cui appartengono i tuoi account.

Abilitazione di AWS Config

Consulta la seguente documentazione:

- Documentazione AWS Config
- Prezzi di AWS Config
- Abilitazione di AWS Config

Abilita AWS Config in entrambi gli account e in entrambe le regioni. Ciò comporterà dei costi.

> **Important**
>
> Assicurati di scegliere l'opzione «Includi risorse globali (come le risorse AWS IAM)». Se non scegli questa opzione quando abiliti AWS Config, non vedrai i risultati relativi alle risorse globali (come le risorse AWS IAM).

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Abilitazione di AWS Config	Abilitazione di AWS Config
222222222222	Membro	Abilitazione di AWS Config	Abilitazione di AWS Config

Abilita AWS Security Hub

Consulta la seguente documentazione:

- Documentazione AWS Security Hub
- Prezzi di AWS Security Hub
- Abilitazione di AWS Security Hub

Abilita AWS Security Hub in entrambi gli account e in entrambe le regioni. Ciò comporterà dei costi.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Abilita AWS Security Hub	Abilita AWS Security Hub
222222222222	Membro	Abilita AWS Security Hub	Abilita AWS Security Hub

Abilita risultati di controllo consolidati

Consulta la seguente documentazione:

- Generazione e aggiornamento dei risultati di controllo

Ai fini di questo tutorial, dimostreremo l'utilizzo della soluzione con la funzionalità consolidata dei risultati di controllo di AWS Security Hub abilitata, che è la configurazione consigliata. Nelle partizioni che non supportano questa funzionalità al momento della scrittura, dovrai distribuire i playbook specifici dello standard anziché SC (Security Control).

Abilita i risultati di controllo consolidati in entrambi gli account e in entrambe le regioni.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Abilita risultati di controllo consolidati	Abilita risultati di controllo consolidati
222222222222	Membro	Abilita risultati di controllo consolidati	Abilita risultati di controllo consolidati

La generazione dei risultati con la nuova funzionalità potrebbe richiedere del tempo. Puoi procedere con il tutorial, ma non puoi correggere i risultati generati senza la nuova funzionalità. I risultati generati con la nuova funzionalità possono essere identificati dal valore `security-control/<control_id>` del `GeneratorId` campo.

Configura l'aggregazione dei risultati tra regioni

Consulta la seguente documentazione:

- Cross-Region aggregazione
- Abilitare l'aggregazione interregionale

Configura l'aggregazione dei risultati da us-west-2 a us-east-1 in entrambi gli account.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Configura l'aggregazione da us-west-2	Nessuno
222222222222	Membro	Configura l'aggregazione da us-west-2	Nessuno

Potrebbe essere necessario del tempo prima che i risultati si propaghino nella regione di aggregazione. Puoi procedere con il tutorial, ma non potrai correggere i risultati di altre regioni finché non inizieranno a comparire nella regione di aggregazione.

Designare un account amministratore di Security Hub

Consulta la seguente documentazione:

- Gestione degli account in AWS Security Hub
- Gestione degli account dei membri dell'organizzazione
- Gestione degli account dei membri tramite invito

Nell'esempio precedente, questo tutorial utilizza il metodo di invito manuale. Per un set di account di produzione, consigliamo di gestire l'amministrazione delegata di Security Hub tramite AWS Organizations.

Dalla console di AWS Security Hub nell'account admin (111111111111), invita l'account membro (222222222222) ad accettare l'account amministratore come amministratore delegato di Security Hub. Dall'account membro, accetta l'invito.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Invita l'account del membro	Nessuno
222222222222	Membro	Accetta l'invito	Nessuno

La propagazione dei risultati all'account amministratore potrebbe richiedere del tempo. Puoi procedere con il tutorial, ma non potrai correggere i risultati degli account dei membri finché non inizieranno a comparire nell'account amministratore.

Crea i ruoli per le autorizzazioni StackSets autogestite

Consulta la seguente documentazione:

- AWS CloudFormation StackSets
- Concedi autorizzazioni autogestite

Distribuiremo gli CloudFormation stack su più account, quindi utilizzeremo. StackSets Non possiamo utilizzare le autorizzazioni gestite dal servizio perché lo stack di amministrazione e lo stack dei membri hanno stack annidati, che non sono supportati dal servizio, quindi dobbiamo utilizzare autorizzazioni autogestite.

Distribuisci gli stack per le autorizzazioni di base per le operazioni. StackSet Per gli account di produzione, potresti voler restringere le autorizzazioni in base alla documentazione sulle «opzioni di autorizzazione avanzate».

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Implementa lo stack di ruoli di amministratore StackSet Distribuisci lo stack di ruoli StackSet Execution	Nessuno

Account	Scopo	Azione in us-east-1	Azione in us-west-2
222222222222	Membro	Distribuisci lo stack dei ruoli di StackSet esecuzione	Nessuno

Crea le risorse non sicure che genereranno risultati di esempio

Consulta la seguente documentazione:

- Riferimento ai controlli Security Hub
- Controlli AWS Lambda

Quanto segue crea una risorsa di esempio con una configurazione non sicura per dimostrare una soluzione. Il controllo di esempio è Lambda.1: le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico.

> **Important**
>
> Creerai intenzionalmente una risorsa con una configurazione non sicura. Esamina la natura del controllo e valuta il rischio di creare tale risorsa nel tuo ambiente. Siate consapevoli degli strumenti di cui la vostra organizzazione potrebbe disporre per rilevare e segnalare tali risorse e richiedete un'eccezione, se necessario. Se il controllo di esempio non è appropriato per il tuo ambiente, seleziona un altro controllo supportato dalla soluzione.

Nella seconda regione dell'account membro, accedi alla console AWS Lambda e crea una funzione nell'ultimo runtime di Python. In Configurazione → Autorizzazioni, aggiungi una dichiarazione di policy per consentire di richiamare la funzione dall'URL senza autenticazione.

Conferma nella pagina della console che la funzione consenta l'accesso pubblico. Dopo che la soluzione ha risolto il problema, confronta le autorizzazioni per confermare che l'accesso pubblico è stato revocato.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Nessuno	Nessuno

Account	Scopo	Azione in us-east-1	Azione in us-west-2
222222222222	Membro	Nessuno	Crea una funzione Lambda con una configurazione non sicura

AWS Config potrebbe impiegare del tempo per rilevare la configurazione non sicura. Puoi procedere con il tutorial, ma non potrai porre rimedio alla scoperta finché Config non la rileverà.

Crea gruppi di CloudWatch log per i controlli correlati

Consulta la seguente documentazione:

- Monitoraggio dei file di CloudTrail log con Amazon CloudWatch Logs
- CloudTrail controlli

CloudTrail I vari controlli supportati dalla soluzione richiedono la presenza di un gruppo di CloudWatch log che sia la destinazione di un gruppo multiregionale CloudTrail. Nel seguente esempio, creeremo un gruppo di log segnaposto. Per gli account di produzione, è necessario configurare correttamente CloudTrail l'integrazione con CloudWatch Logs.

Crea un gruppo di log in ogni account e regione con lo stesso nome, ad esempio:`asr-log-group`.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Creazione di un gruppo di log	Creazione di un gruppo di log
222222222222	Membro	Creazione di un gruppo di log	Creazione di un gruppo di log

Distribuisci la soluzione sugli account dei tutorial

Raccogli i tre URL di Amazon S3 per lo stack dei ruoli di amministratore, membro e membro.

Implementa lo stack di amministrazione

View template automa

security-response-admin.template

Nell'account amministratore, accedi alla CloudFormation console e distribuisci lo stack di amministrazione nella regione di aggregazione dei risultati di Security Hub.

Scegli `No` il valore di tutti i parametri per il caricamento degli stack di amministrazione annidati ad eccezione dello stack «SC» o «Security Control». Questo stack contiene le risorse per i risultati di controllo consolidati che abbiamo configurato nei nostri account.

Scegli `No` di riutilizzare il gruppo di log di orchestrator a meno che tu non abbia già implementato questa soluzione in questo account e in questa regione.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
`111111111111`	Admin	Implementa lo stack di amministrazione	Nessuno
`222222222222`	Membro	Nessuno	Nessuno

Dovresti ricevere uno `CREATE_COMPLETE` stato nella CloudFormation console AWS.

Attendi che lo stack di amministrazione completi la distribuzione prima di continuare, in modo da poter creare una relazione di fiducia dagli account dei membri all'account amministratore.

Distribuisci lo stack di membri

View template automa

security-response-member.template

Nell'account amministratore, accedi alla CloudFormation StackSets console e distribuisci lo stack di membri in ogni account e regione. Usa i ruoli di StackSets amministrazione ed esecuzione creati in questo tutorial.

Inserisci il nome del gruppo di log che hai creato come valore per il parametro per il nome del gruppo di log.

Scegliete No il valore di tutti i parametri per il caricamento degli stack di membri annidati ad eccezione dello stack «SC» o «security control». Questo stack contiene le risorse per i risultati di controllo consolidati che abbiamo configurato nei nostri account.

Inserisci l'ID dell'account amministratore come valore per il parametro per il numero dell'account amministratore. Nel nostro esempio, questo è`111111111111`.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
`111111111111`	Admin	Distribuisci il membro StackSet /Conferma lo stack di membri distribuito	Conferma lo stack di membri distribuito
`222222222222`	Membro	Conferma lo stack di membri distribuito	Conferma lo stack di membri distribuito

Dovresti ricevere uno `CREATE_COMPLETE` stato per ogni istanza dello stack nella CloudFormation StackSets console AWS.

Distribuisci lo stack dei ruoli dei membri

automated-security-response-member-roles.template pulsante automated-security-response-member-roles.template

Nell'account amministratore, accedi alla console e distribuisci lo stack di membri su ciascun account. CloudFormation StackSets Usa i ruoli di StackSets amministrazione ed esecuzione creati in questo tutorial. Inserisci l'ID dell'account amministratore come valore per il parametro per il numero dell'account amministratore. Nel nostro esempio, questo è`111111111111`.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
`111111111111`	Admin	Distribuisci il membro StackSet /Conferma	Nessuno

Account	Scopo	Azione in us-east-1	Azione in us-west-2
		lo stack di membri distribuito	
222222222222	Membro	Conferma lo stack di membri distribuito	Nessuno

Dovresti ricevere uno `CREATE_COMPLETE` stato per ogni istanza dello stack nella CloudFormation StackSets console AWS.

Puoi procedere, ma non potrai correggere i risultati fino al CloudFormation StackSets termine della distribuzione.

Iscriviti all'argomento SNS

Aggiornamenti relativi alle correzioni

Argomento - SO0111-ASR _Argomento

Nell'account amministratore, iscriviti all'argomento Amazon SNS creato dallo stack di amministrazione. Questo ti avvisa quando le correzioni vengono avviate e quando hanno esito positivo o negativo.

Allarmi

Argomento - _ SO0111-ASR Alarm_Topic

Nell'account amministratore, iscriviti all'argomento Amazon SNS creato dallo stack di amministrazione. Questo ti avviserà quando si attivano gli allarmi metrici.

Correggi i risultati degli esempi

> **Important**
>
> Questo esempio richiede l'uso della console Security Hub CSPM. La console Security Hub (non CSPM) attualmente non supporta le correzioni manuali tramite azioni personalizzate. Per correggere i risultati senza utilizzare la console Security Hub CSPM, consulta la sezione Correggere utilizzando l'interfaccia utente Web.

Nell'account amministratore, accedi alla console CSPM di Security Hub e individua il risultato della risorsa con una configurazione non sicura che hai creato come parte di questo tutorial.

Questa operazione può essere eseguita in diversi modi:

1. Nelle partizioni che supportano la funzionalità dei risultati di controllo consolidati, una pagina denominata «Controlli» consente di individuare i risultati in base all'ID di controllo consolidato.
2. Nella pagina «Standard di sicurezza», è possibile individuare il controllo in base allo standard a cui appartiene.
3. Puoi visualizzare tutti i risultati nella pagina «Risultati» e cercare per attributo.

L'ID di controllo consolidato per la funzione Lambda pubblica che abbiamo creato è. Lambda.1

Avvia la riparazione

Seleziona la casella di controllo a sinistra del risultato relativo alla risorsa che abbiamo creato. Nel menu a discesa «Azioni», seleziona «Correggi con ASR». Vedrai una notifica indicante che il risultato è stato inviato ad Amazon. EventBridge

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Avviare la riparazione	Nessuno
222222222222	Membro	Nessuno	Nessuno

Conferma che la riparazione ha risolto il problema

Dovresti ricevere due notifiche SNS. La prima indicherà che è stata avviata una riparazione e la seconda indicherà che la riparazione è riuscita. Dopo aver ricevuto la seconda notifica, accedi alla console Lambda nell'account del membro e conferma che l'accesso pubblico è stato revocato.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Nessuno	Nessuno
222222222222	Membro	Nessuno	Conferma che la riparazione è riuscita

Correggi utilizzando l'interfaccia utente Web

In alternativa, puoi utilizzare l'interfaccia utente Web della soluzione per correggere i risultati di AWS Security Hub e visualizzare le correzioni precedenti.

> **Note**
>
> È necessario impostare il `ShouldDeployWebUI` parametro su «sì» quando si distribuisce lo stack di amministrazione per utilizzare l'interfaccia utente Web della soluzione.

Accedere all'interfaccia utente Web

Dopo aver distribuito la soluzione, riceverai un'e-mail con credenziali temporanee e un link all'interfaccia utente Web della soluzione da no-reply@verificationemail.com. Questo verrà inviato all'indirizzo email che hai fornito durante la distribuzione dello stack di amministrazione.

Individua l'email, copia le credenziali temporanee e scegli il collegamento all'interfaccia utente Web. Questo link ti porterà direttamente alla pagina di accesso, dove inserirai le tue credenziali temporanee e imposterai una nuova password.

Individua il risultato Lambda.1

Una volta effettuato l'accesso, ti verrà presentata la pagina dei risultati. Questa pagina mostra tutti i risultati di Security Hub nel tuo account amministratore di Security Hub che sono supportati per la correzione, inclusi i risultati per gli account membri integrati in AWS Security Hub.

Nella pagina Risultati, utilizza la barra di ricerca per filtrare in base all'ID della risorsa inserendo l'ARN della funzione Lambda creata come parte di questo tutorial ed eseguendo una ricerca utilizzando l'operatore «=». Verranno visualizzati tutti i risultati di AWS Security Hub supportati dalla soluzione per la funzione Lambda creata.

Per `Lambda.1` trovare i risultati generati in questo tutorial, applica un altro filtro su Finding Type. Scegli la barra di ricerca, seleziona Tipo di ricerca e seleziona l'operatore «=». Se i risultati di controllo consolidati sono abilitati nel tuo ambiente, inserisci`security-control/Lambda.1`. Altrimenti, scegli uno standard di sicurezza che supporti il Lambda.1 controllo e inserisci il Generator ID, ad esempio`aws-foundational-security-best-practices/v/1.0.0/Lambda.1`.

Dopo aver applicato i filtri Resource ID e Finding Type, nella tabella vedrai solo i Lambda.1 risultati generati da AWS Security Hub per la tua risorsa di test.

> **Note**
>
> AWS Security Hub potrebbe impiegare del tempo per generare il Lambda.1 risultato della risorsa creata. Se non vedi il risultato dopo aver applicato entrambi i filtri, attendi 5-10 minuti e cerca nuovamente il risultato.

Avvia la riparazione

Seleziona la scoperta che hai trovato nel passaggio precedente, quindi scegli Azioni > Correggi. Verrà avviata la correzione del risultato selezionato.

È possibile visualizzare lo stato di avanzamento di questa correzione nella pagina Cronologia delle esecuzioni. Dopo aver atteso qualche minuto, aggiorna la pagina Cronologia delle esecuzioni scegliendo l'icona di aggiornamento in alto a destra e dovresti vedere che lo stato è cambiato da a. `In progress` `Success`

Conferma che la correzione ha risolto il problema

Quando il risultato viene contrassegnato come `Resolved` da AWS Security Hub, verrà automaticamente rimosso dalla pagina Risultati nell'interfaccia utente Web.

Per verificare che la correzione abbia risolto il risultato, accedi alla console Lambda nell'account del membro e conferma che l'accesso pubblico è stato revocato.

> **Note**
>
> Alcuni risultati potrebbero comunque essere visualizzati nella pagina Risultati anche con lo stato di riparazione pari a. `Success` Questo perché AWS Security Hub impiega fino a 24 ore per contrassegnare un risultato come risolto dopo l'aggiornamento della risorsa. Puoi eliminare i risultati che non desideri più visualizzare nella pagina Risultati selezionando il risultato e scegliendo Azioni > Elimina.

Correggi in batch un arretrato di risultati utilizzando l'API

L'interfaccia utente Web e l'azione personalizzata CSPM di AWS Security Hub sono utili per correggere un numero limitato di rilevazioni in modo interattivo. Per elaborare un ampio backlog di

risultati esistenti in modo programmatico, ad esempio subito dopo l'implementazione della soluzione, chiama direttamente l'API REST della soluzione.

La stessa API REST che supporta l'interfaccia utente Web (denominata AutomatedSecurityResponseApi nella console API Gateway) espone un `POST /findings/action` endpoint che accetta un batch di risultati da correggere in un'unica richiesta. Ciò consente di correggere un arretrato tramite script anziché selezionare manualmente i risultati.

> **Note**
>
> Questo endpoint è disponibile solo quando l'interfaccia utente Web è abilitata (distribuisci lo stack di amministrazione con «sì» `ShouldDeployWebUI` impostato su «sì»). Puoi trovare l'URL di richiamo dell'API per la `prod` fase nella console API Gateway per l'API. AutomatedSecurityResponseApi

Autentica

Tutte le richieste API richiedono un token di accesso Amazon Cognito emesso per il pool di utenti della soluzione, passato nell'`Authorization`intestazione come token al portatore. Il token deve contenere l'ambito. `asr-api/api` Utilizza un token per uno dei ruoli della soluzione (amministratore, amministratore delegato o operatore dell'account); la stessa autorizzazione basata sui ruoli che si applica nell'interfaccia utente Web si applica all'API. Per l'automazione automatica, ottieni un token utilizzando il flusso OAuth da macchina a macchina (credenziali del cliente) anziché un accesso utente interattivo.

Raccogli i risultati per porvi rimedio

`POST /findings`Utilizzalo per cercare e sfogliare i risultati che desideri correggere e raccogli quelli `findingId` di ciascuno. I risultati restituiti si riferiscono agli account per i quali il ruolo è autorizzato, pertanto un Account Operator riceve solo i risultati relativi agli account assegnati.

Chiama l'endpoint dell'azione dei risultati

Invia gli ID dei risultati raccolti a `POST /findings/action` with an `actionType` of`Remediate`. Ogni risultato viene indirizzato all'Orchestrator esattamente come dall'interfaccia utente Web.

```
POST /findings/action
```

```
Authorization: Bearer <access-token>
Content-Type: application/json

{
  "actionType": "Remediate",
  "findingIds": [
    "arn:aws:securityhub:us-east-1:111111111111:security-control/Lambda.1/finding/...",
    "arn:aws:securityhub:us-east-1:111111111111:security-control/S3.5/finding/..."
  ]
}
```

`actionType`accetta anche `RemediateAndGenerateTicket` (correggi e apri un ticket nel canale di ticketing configurato) e`Suppress`/`Unsuppress`per modificare lo stato del flusso di lavoro di Security Hub di un risultato. Una `RemediateAndGenerateTicket` richiesta `Remediate` o restituisce HTTP `202` con il corpo di`{"status": "IN_PROGRESS"}`; `Suppress` e `Unsuppress` restituisce HTTP. `200`

> **Important**
>
> Invia al massimo 50 ID di ricerca per richiesta. Per rimediare a un arretrato maggiore, suddividi gli ID di ricerca in batch di 50 o meno ed invia una richiesta per batch. L'API è inoltre protetta da regole basate sulla frequenza (vedi la configurazione AWS WAF in API Gateway Security Policy), quindi procedi con batch successivi anziché inviarli tutti in una volta.

Monitoraggio dell'avanzamento

Le correzioni avviate tramite l'API vengono eseguite in modo asincrono, proprio come quelle avviate dall'interfaccia utente Web. Monitora i loro progressi nella pagina Cronologia delle esecuzioni dell'interfaccia utente Web, tramite le notifiche Amazon SNS della soluzione o interrogando. `POST /remediations`

Tieni traccia dell'esecuzione della correzione

Per comprendere meglio come funziona la soluzione, è possibile tracciare l'esecuzione della riparazione.

EventBridge regola

Nell'account amministratore, individua una EventBridge regola denominata Remediate_with_ASR_CustomAction. Questa regola corrisponde ai risultati inviati da Security Hub e li invia a Orchestrator Step Functions.

Esecuzione Step Functions

Nell'account amministratore, individua le AWS Step Functions denominate "SO0111-ASR-Orchestrator». Questa funzione Step richiama il documento SSM Automation nell'account e nella regione di destinazione. Puoi tracciare l'esecuzione della correzione nella cronologia delle esecuzioni di questo AWS Step Functions.

Automazione SSM

Nell'account membro, accedi alla console di SSM Automation. Troverai due esecuzioni di un documento denominato "ASR-SC_2.0.0_" e un'esecuzione di un documento denominato Lambda.1 "». ASR-RemoveLambdaPublicAccess

La prima esecuzione proviene dalla funzione Orchestrator Step nell'account di destinazione. La seconda esecuzione avviene nella regione di destinazione, che potrebbe non essere la regione da cui ha avuto origine il risultato. L'esecuzione finale è la correzione che revoca la politica di accesso pubblico dalla Lambda Function.

CloudWatch Log Group

Nell'account amministratore, accedi alla console CloudWatch Logs e individua un gruppo di log denominato "SO0111-ASR». Questo gruppo di log è la destinazione per l'output del Remediation Runbook. Per i log di Orchestrator Step Functions, fare riferimento al gruppo di log "». SO0111-ASR-Orchestrator

Abilita correzioni completamente automatiche

L'altra modalità operativa della soluzione consiste nel correggere automaticamente i risultati non appena arrivano in Security Hub.

> **Important**
>
> Prima di abilitare le correzioni completamente automatiche, verifica che la soluzione sia configurata negli account e nelle regioni in cui desideri che la soluzione apporti modifiche

automatiche. Per restringere l'ambito delle correzioni automatiche della soluzione, vedi Filtrare le correzioni completamente automatiche.

Note

I risultati eliminati in AWS Security Hub non vengono corretti automaticamente, anche quando è abilitata una correzione completamente automatica per il controllo corrispondente. Un risultato viene eliminato quando lo stato del flusso di lavoro è. `SUPPRESSED` La soluzione ignora i risultati eliminati durante l'avvio automatico, quindi la soppressione di un risultato in Security Hub è un modo efficace per escludere risultati specifici dalla correzione automatica lasciando il controllo abilitato. I risultati eliminati possono ancora essere corretti su richiesta dall'interfaccia utente Web o dall'azione personalizzata CSPM di AWS Security Hub.

Limite di tentativi di correzione automatica

Quando una correzione completamente automatica fallisce, AWS Security Hub reimporta i risultati ancora non risolti, altrimenti la soluzione attiverebbe nuovamente la correzione a tempo indeterminato. Per evitare che ciò accada, la soluzione riprova una ricerca non riuscita per un massimo di 3 volte, attendendo almeno 15 minuti tra un tentativo e l'altro. Dopo il terzo tentativo, la soluzione interrompe automaticamente il tentativo di ricerca ed emette la `RemediationRetryCapReached` metrica Amazon. CloudWatch Il risultato rimane visibile nella soluzione e può ancora essere corretto su richiesta dall'interfaccia utente Web o dall'azione personalizzata CSPM di AWS Security Hub. Questo limite si applica per risultato e non influisce su altri risultati o controlli.

Esempio: abilita correzioni completamente automatiche per Lambda.1

L'attivazione delle correzioni automatiche avvierà le correzioni su tutte le risorse corrispondenti al controllo abilitato (). Lambda.1

Important

Conferma che desideri che questa autorizzazione venga revocata a tutte le funzioni Lambda pubbliche incluse nell'ambito della soluzione. Le correzioni completamente automatiche non

saranno limitate alla funzione creata. La soluzione porrà rimedio a questo controllo se viene rilevato in uno qualsiasi degli account e delle regioni in cui è installata.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Conferma l'assenza di funzioni pubbliche desiderate	Conferma l'assenza di funzioni pubbliche desiderate
222222222222	Membro	Conferma l'assenza di funzioni pubbliche desiderate	Conferma l'assenza di funzioni pubbliche desiderate

Individua la tabella DynamoDB di configurazione della riparazione

Nell'account Admin, visualizza lo stack `Outputs` di amministrazione nella console. CloudFormation Vedrai un output intitolato`RemediationConfigurationDynamoDBTable`.

Questo è il nome della tabella Remediation Configuration DynamoDB, che controlla le configurazioni di riparazione automatiche per la soluzione. Copia il valore di questo output e individua la tabella DynamoDB corrispondente nella console DynamoDB. https://console.aws.amazon.com/dynamodbv2/

migrazione da v2 a v4

Se è stato eseguito l'aggiornamento dalla versione 2.x alla versione 4.0.0 o successiva, la soluzione compila automaticamente questa tabella con i controlli per i quali è stata abilitata la correzione automatica nella versione 2. Gli elementi scritti dalla migrazione sono `modifiedBy` impostati su`v2-migration`, in modo da poter distinguere le voci migrate dalle modifiche manuali. Per verificare che la migrazione sia avvenuta correttamente per i controlli previsti, interroga la tabella `automatedRemediationEnabled = true` ed esamina il risultato. Tutti i controlli ignorati durante la migrazione (regole CIS senza una correzione ASR nella v2 o controlli v3+ non forniti) devono essere abilitati manualmente utilizzando la procedura seguente. Per informazioni dettagliate sull'esito della migrazione, fare riferimento a Aggiornamento della soluzione.

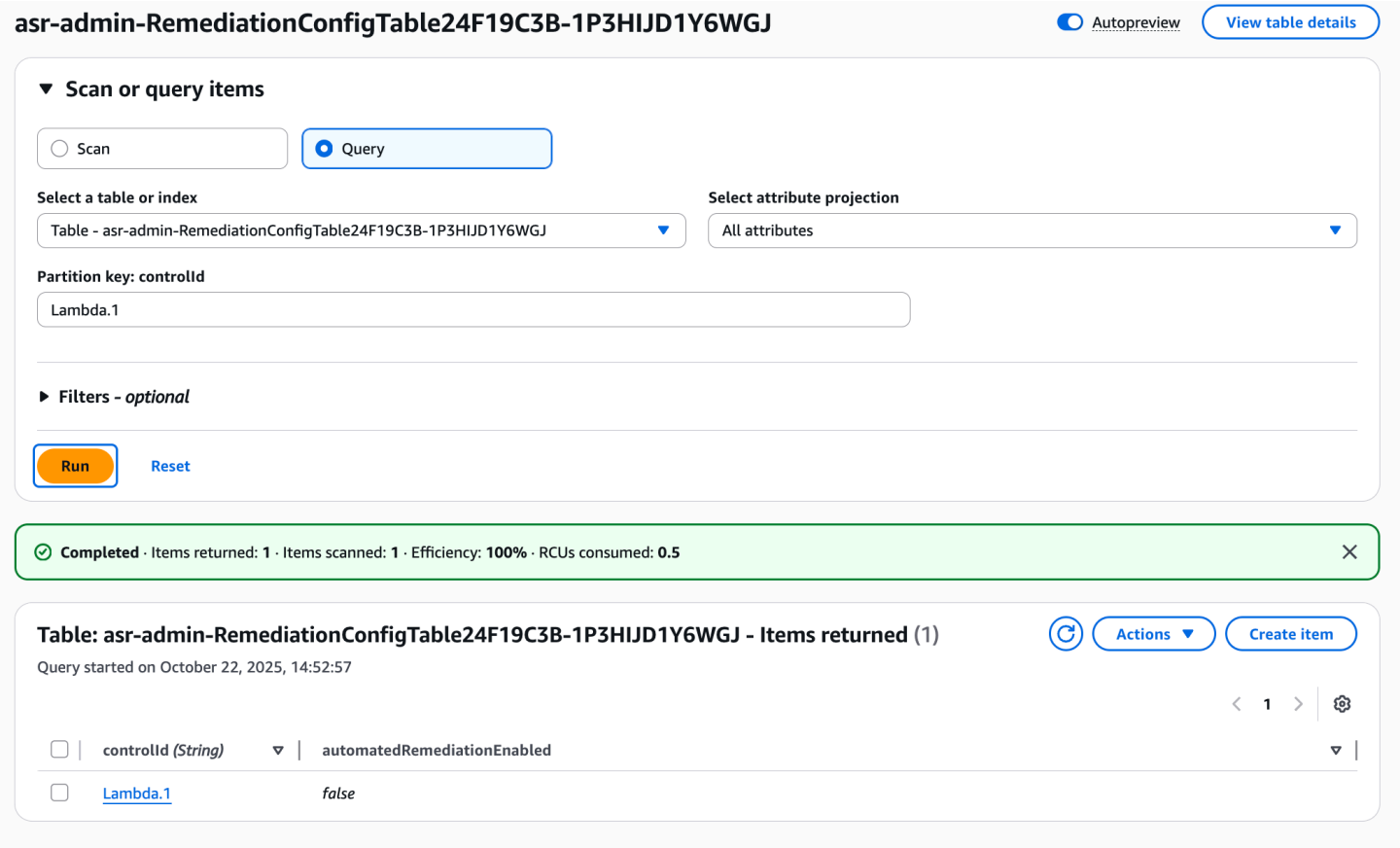
Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Individua la tabella Remediation Configuration DynamoDB.	Nessuno
222222222222	Membro	Nessuno	Nessuno

Modificare la tabella di configurazione della riparazione

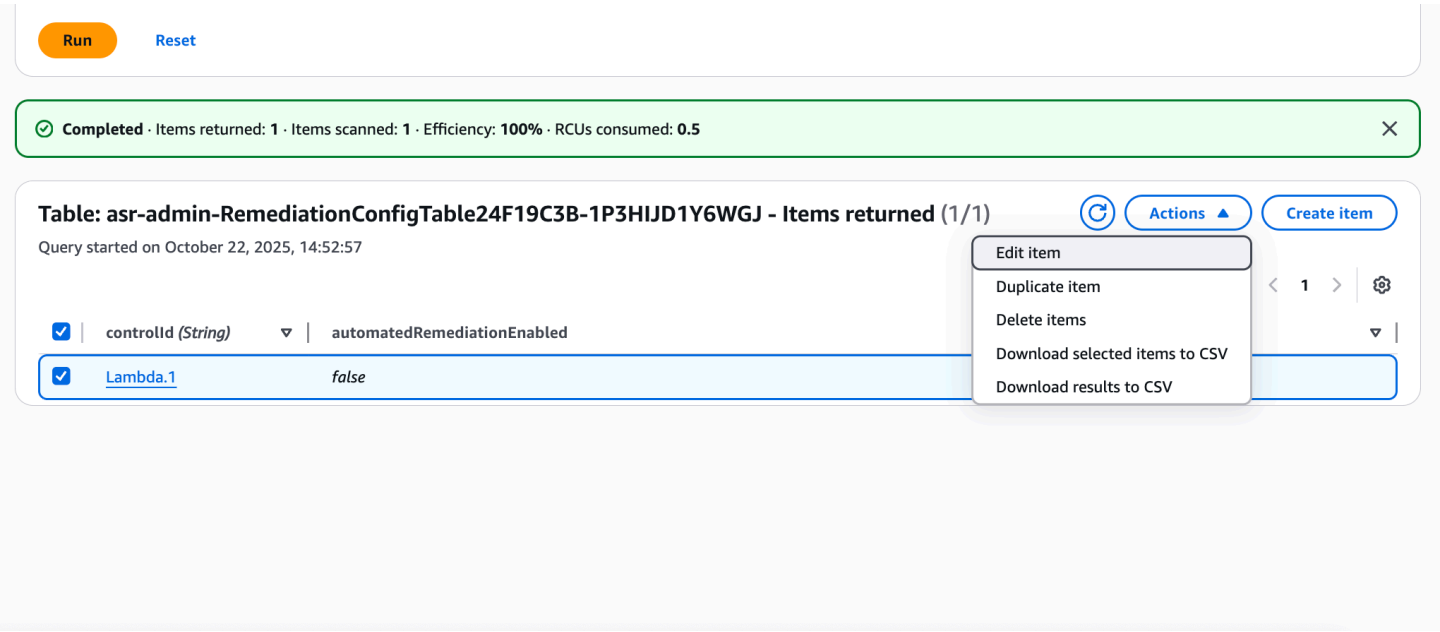
Nella console DynamoDB in cui hai posizionato la tabella di configurazione della riparazione, scegli Esplora elementi della tabella.

Ogni elemento della tabella corrisponde a un controllo Security Hub supportato dalla soluzione. Ogni elemento ha un `automatedRemediationEnabled` attributo che può essere modificato per abilitare correzioni completamente automatiche per il controllo associato.

Per abilitarlo Lambda.1, in Elementi di scansione o interrogazione scegli Interrogazione. In Chiave di partizione: ControlID, inserisci `Lambda.1` e scegli Esegui. Verrà restituito un singolo elemento corrispondente al Lambda.1 controllo.



Ora seleziona l'`Lambda.1`elemento, quindi scegli Azioni > Modifica elemento.



Infine, modifica il valore dell'`automatedRemediationEnabled`attributo su True. Scegliete Salva e chiudi.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Modifica la tabella Remediation Configuration DynamoDB.	Nessuno
222222222222	Membro	Nessuno	Nessuno

Configura la risorsa

Nell'account membro, riconfigura la funzione Lambda per consentire l'accesso pubblico.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Nessuno	Nessuno
222222222222	Membro	Nessuno	Configura la funzione Lambda per consentire l'accesso pubblico

Conferma che la correzione ha risolto il problema

Potrebbe essere necessario del tempo prima che Config rilevi nuovamente la configurazione non sicura. Dovresti ricevere due notifiche SNS. La prima indicherà che è stata avviata una riparazione. Il secondo indicherà che la riparazione è avvenuta con successo. Dopo aver ricevuto la seconda notifica, accedi alla console Lambda nell'account del membro e conferma che l'accesso pubblico è stato revocato.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Nessuno	Nessuno
222222222222	Membro	Nessuno	Conferma che la riparazione è riuscita

(Facoltativo) Filtrare le correzioni completamente automatiche

Per limitare l'ambito in cui la soluzione esegue correzioni completamente automatiche, applica filtri sulle risorse. I filtri si applicano solo alle correzioni completamente automatizzate e non influiscono sulle correzioni avviate manualmente.

Un filtro delle risorse è una definizione riutilizzabile che definisce gli ambiti ai quali risultati vengono corretti automaticamente. Ogni filtro può combinare gli ID degli account, le unità organizzative (OU) di AWS Organizations, i modelli ARN delle risorse e i tag delle risorse. È possibile creare filtri nella pagina Filtri dell'interfaccia utente Web, quindi applicarli a un singolo controllo dalla pagina Controlli (o a tutti i controlli contemporaneamente) utilizzando la modalità Includi o Escludi.

Per una procedura dettagliata completa, inclusa la creazione di filtri, l'applicazione ai controlli e il modo in cui la soluzione valuta le modalità di inclusione ed esclusione, vedi Creare e applicare filtri per le risorse nella guida per l'amministratore.

Eliminazione

Elimina le risorse di esempio

Nell'account membro, elimina la funzione Lambda di esempio che hai creato.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Nessuno	Nessuno
222222222222	Membro	Nessuno	Elimina l'esempio della funzione Lambda

Elimina lo stack di amministrazione

Nell'account amministratore, elimina lo stack di amministrazione.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Elimina lo stack di amministrazione	Nessuno

Account	Scopo	Azione in us-east-1	Azione in us-west-2
222222222222	Membro	Nessuno	Nessuno

Elimina lo stack di membri

Nell'account Admin, elimina il membro StackSet.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Elimina il membro StackSet Conferma l'elimina zione dello stack di membri	Conferma l'elimina zione dello stack di membri
222222222222	Membro	Conferma l'elimina zione dello stack di membri	Conferma l'elimina zione dello stack di membri

Elimina lo stack dei ruoli dei membri

Nell'account Admin, elimina i ruoli dei membri StackSet.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Elimina i ruoli dei membri StackSet Conferma l'elimina zione dello stack dei ruoli dei membri	Nessuno
222222222222	Membro	Conferma l'elimina zione dello stack dei ruoli dei membri	Nessuno

Elimina i ruoli mantenuti

In ogni account, elimina i ruoli IAM mantenuti.

Importante: questi ruoli vengono mantenuti per le correzioni che richiedono un ruolo affinché la correzione continui a funzionare (ad esempio, la registrazione del flusso VPC). Conferma di non richiedere il funzionamento continuo di nessuno di questi ruoli prima di eliminarli.

Eliminare tutti i ruoli con il prefisso SO0111-.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Elimina i ruoli mantenuti	Nessuno
222222222222	Membro	Eliminare i ruoli mantenuti	Nessuno

Pianifica l'eliminazione delle chiavi AWS KMS conservate

Gli stack di amministratori e membri creano e conservano una chiave AWS KMS. Se conservi queste chiavi, ti verranno addebitati dei costi.

Queste chiavi vengono conservate per consentirti di accedere a tutte le risorse crittografate dalla soluzione. Conferma di non averne bisogno prima di programmarne l'eliminazione.

Identifica le chiavi distribuite dalla soluzione utilizzando gli alias creati dalla soluzione o dalla cronologia. CloudFormation Pianificane l'eliminazione.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Identifica e pianifica la chiave di amministrazione per l'eliminazione Identifica e pianifica la chiave membro per l'eliminazione	Identifica e pianifica la chiave membro per l'eliminazione

Account	Scopo	Azione in us-east-1	Azione in us-west-2
222222222222	Membro	Identifica e pianifica la chiave membro per l'eliminazione	Identifica e pianifica la chiave membro per l'eliminazione

Elimina gli stack per le autorizzazioni autogestite StackSets

Elimina gli stack creati per consentire le autorizzazioni autogestite StackSets

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Elimina lo stack dei ruoli StackSet dell'amministratore	Nessuno
222222222222	Membro	Eliminare lo stack StackSet dei ruoli di esecuzione	Nessuno

Guida per sviluppatori

Questa sezione fornisce il codice sorgente per la soluzione e personalizzazioni aggiuntive.

Codice sorgente

Visita il nostro GitHub archivio per scaricare i modelli e gli script per questa soluzione e condividere le tue personalizzazioni con altri.

Playbook

Questa soluzione include le correzioni per gli standard di sicurezza definiti come parte del Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v3.0.0, AWS Foundational Security Best Practices (FSBP) v1.0.0 , Payment Card Industry Data Security Standard () v3.2.1 e National Institute of Standards and Technology (PCI-DSSNIST). https://docs.aws.amazon.com/securityhub/latest/userguide/nist-standard.html

Se hai abilitato i risultati di controllo consolidati, tali controlli sono supportati in tutti gli standard. Se questa funzionalità è abilitata, è necessario implementare solo il playbook SC. In caso contrario, i playbook sono supportati per gli standard elencati in precedenza.

> **Important**
>
> Implementa i playbook solo per gli standard abilitati per evitare di raggiungere le quote di servizio.

Per i dettagli su una soluzione specifica, consulta il documento di automazione di Systems Manager con il nome distribuito dalla soluzione nel tuo account. Vai alla console di AWS Systems Manager, quindi nel pannello di navigazione scegli Documents.

Description	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
Correzioni totali	63	34	29	33	65	19	90
ASR-EnableAutoScalingGroupELBHealthCheck I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità del sistema di bilanciamento del carico	AutoScaling.1		AutoScaling.1		AutoScaling.1		AutoScaling.1

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-ConfigureAutoScalingLaunchConfigToRequireIMDSv2 Le configurazioni di avvio dei gruppi Auto Scaling dovrebbero configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)					AutoScaling.3		AutoScaling.3

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Creat eCloudTra ilMultiRe gionTrail CloudTrai l devono essere attivate e configura te con almeno un percorso multiregi onale	CloudTrai l.1	2.1	CloudTrai l.2	3.1	CloudTrai l.1	3.1	CloudTrai l.1
ASR-Enabl eEncrypti on CloudTrai l dovrebbe essere attivata la crittogra fia a riposo	CloudTrai l.2	2.7	CloudTrai l.1	3.7	CloudTrai l.2	3.5	CloudTrai l.2

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eLogFileV alidation Assicurat i che la convalida dei file di CloudTrai l registro sia attivata	CloudTrai l.4	2.2	CloudTrai l.3	3.2	CloudTrai l.4		CloudTrai l.4
ASR-Enabl eCloudTra ilToCloud WatchLogg ing Assicurat i che i CloudTrai l percorsi siano integrati con Amazon Logs CloudWatc h	CloudTrai l.5	2.4	CloudTrai l.4	3.4	CloudTrai l.5		CloudTrai l.5

Description	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-ConfigureS3BucketLogging Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail		2.6		3.6		3.4	CloudTrail.7

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-ReplaceCodeBuildClearTextCredentials CodeBuild le variabili di ambiente del progetto non devono contenere credenziali in testo non crittografato	CodeBuild.2		CodeBuild.2		CodeBuild.2		CodeBuild.2

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eAWSConf g Assicurati che AWS Config sia attivato	Config.1	2.5	Config.1	3.5	Config.1	3.3	Config.1
ASR-MakeE BSSnapsho tsPrivate Le istantane e di Amazon EBS non devono essere ripristin abili pubblicam ente	EC2.1		EC2.1		EC2.1		EC2.1

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Remov eVPCDefau ltSecurit yGroupRul es Il gruppo di sicurezza predefini to di VPC dovrebbe vietare il traffico in entrata e in uscita	EC2.2	4.3	EC2.2	5.3	EC2.2	5.4	EC2.2

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eVPCFlowL ogs La registraz ione del flusso VPC deve essere abilitata in tutti i VPC	EC2.6	2.9	EC2.6	3.9	EC2.6	3.7	EC2.6
ASR-Enabl eEbsEncry ptionByDe fault La crittogra fia predefini ta EBS dovrebbe essere attivata	EC2.7	2.2.1			EC2.7	2.2.1	EC2.7

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Revok eUnrotate dKeys Le chiavi di accesso degli utenti devono essere ruotate ogni 90 giorni o meno	IAM.3	1.4		1.14	IAM.3	1.14	IAM.3
ASR-SetIA MPasswor Policy Politica di password predefini ta di IAM	IAM.7	1.5-1.11	IAM.8	1.8	IAM.7	1.8	IAM.7

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Revok eUnusedIA MUserCred entials Le credenzia li utente devono essere disattiva te se non utilizzate entro 90 giorni	IAM.8	1.3	IAM.7		IAM.8		IAM.8

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-RevokeUnusedIAMUserCredentials Le credenziali utente devono essere disattivate se non utilizzate entro 45 giorni				1.12		1.12	IAM.22
ASR-RemoveLambdaPublicAccess Le funzioni Lambda dovrebbero vietare l'accesso pubblico	Lambda.1		Lambda.1		Lambda.1		Lambda.1

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-MakeR DSSnapsh tPrivate Le istantane e RDS dovrebber o vietare l'accesso pubblico	RDS.1		RDS.1		RDS.1		RDS.1
ASR-Disab lePublicA ccessToRD SInstance Le istanze DB RDS dovrebber o vietare l'accesso pubblico	RDS.2		RDS.2		RDS.2	2.3.3	RDS.2

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Encry ptRDSSnap shot Le istantane e del cluster RDS e le istantane e del database devono essere crittogra fate quando sono inattive	RDS.4				RDS.4		RDS.4

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eMultiAZO nRDSInsta nce Le istanze DB RDS devono essere configura te con più zone di disponibi lità	RDS.5				RDS.5		RDS.5

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eEnhanced Monitorin gOnRDSIns tance Il monitorag gio avanzato deve essere configura to per le istanze DB e i cluster RDS	RDS.6				RDS.6		RDS.6

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eRDSClust erDeletio nProtecti on La protezion e dall'elim inazione deve essere attivata sui cluster RDS	RDS.7				RDS.7		RDS.7

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eRDSInsta nceDeleti onProtect ion La protezion e dall'elim inazione delle istanze DB RDS deve essere attivata	RDS.8				RDS.8		RDS.8

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eMinorVer sionUpgra deOnRDSI Instance Gli aggiornam enti automatic i delle versioni secondari e di RDS devono essere attivati	RDS.13				RDS.13	2.3.2	RDS.13

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eCopyTags ToSnapsho tOnRDSClu ster I cluster DB RDS devono essere configura ti per copiare i tag nelle istantane e	RDS.16				RDS.16		RDS.16
ASR-Disab lePublicA ccessToRe dshiftClu ster I cluster Amazon Redshift dovrebber o vietare l'accesso pubblico	Redshift. 1		Redshift. 1		Redshift. 1		Redshift. 1

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eAutomati cSnapshot sOnRedshi ftCluster I cluster Amazon Redshift devono avere istantane e automatic he attivate	Redshift. 3				Redshift. 3		Redshift. 3

Description	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-EnableRedshiftClusterAuditLogging I cluster Amazon Redshift devono avere la registrazione di controllo attivata	Redshift.4				Redshift.4		Redshift.4

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eAutomati cVersionU pgradeOnR edshiftCl uster Gli aggiornam enti automatic i alle versioni principal i di Amazon Redshift dovrebber o essere attivati	Redshift. 6				Redshift. 6		Redshift. 6

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Confi gureS3Pub licAccess Block L'imposta zione S3 Block Public Access deve essere attivata	S3.1	2.3	S3.6	2.1.5.1	S3.1	2.1.4	S3.1
ASR-Confi gureS3Buc ketPublic AccessBlo ck I bucket S3 dovrebber o vietare l'accesso pubblico in lettura	S3.2		S3.2	2.1.5.2	S3.2		S3.2

Description	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-ConfigureS3BucketPublicAccessBlock I bucket S3 dovrebbero vietare l'accesso pubblico in scrittura		S3.3					S3.3
ASR-EnableDefaultEncryptionS3 I bucket S3 dovrebbero avere la crittografia lato server attivata	S3.4		S3.4	2.1.1	S3.4		S3.4

Description	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-SetSSLBucketPolicy I bucket S3 dovrebbero richiedere l'utilizzo di SSL	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5

Description	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-S3BlockDenylist Le autorizzazioni Amazon S3 concesse ad altri account AWS nelle policy dei bucket devono essere limitate	S3.6				S3.6		S3.6
L'impostazione S3 Block Public Access deve essere attivata a livello di bucket	S3.8				S3.8		S3.8

Description	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-ConfigureS3BucketPublicAccessBlock Assicurati che il bucket S3 a cui accedi non sia CloudTrail accessibile pubblicamente		2.3					CloudTrail.6

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Creat eAccessLo ggingBuck et Assicurat i che la registraz ione degli accessi al bucket S3 sia attivata sul bucket S3 CloudTrai l		2.6					CloudTrai l.7

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eKeyRotat ion Assicurat i che la rotazione per i CMK creati dal cliente sia attivata		2.8	KMS.1	3.8	KMS.4	3.6	KMS.4

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Creat eLogMetri cFilterAn dAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativam ente alle chiamate API non autorizza te		3.1		4.1			CloudWatc h.1

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Creat eLogMetri cFilterAn dAlarm Assicurat i che esistano un filtro metrico di log e un allarme per l'accesso alla Console di gestione AWS senza MFA		3.2		4.2			CloudWatc h.2

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Creat eLogMetri cFilterAn dAlarm Assicurat i che esistano un filtro metrico di log e un allarme per l'utilizzo da parte dell'uten te «root»		3.3	CW.1	4.3			CloudWatc h.3

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Creat eLogMetri cFilterAn dAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativam ente alle modifiche apportate alle policy IAM		3.4		4.4			CloudWatc h.4

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Creat eLogMetri cFilterAn dAlarm Assicurat i che esistano un filtro metrico di registro e un allarme per le modifiche CloudTrai l alla configura zione		3.5		4.5			CloudWatc h.5

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Creat eLogMetri cFilterAn dAlarm Assicurat i che esistano un filtro metrico di log e un allarme per gli errori di autentica zione della Console di gestione AWS		3.6		4.6			CloudWatc h.6

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Creat eLogMetri cFilterAn dAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativam ente alla disabilit azione o all'elimi nazione pianifica ta delle chiavi gestite dal cliente (CMK) create dal cliente		3.7		4.7			CloudWatc h.7

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Creat eLogMetri cFilterAn dAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativam ente alle modifiche apportate alle policy dei bucket S3		3.8		4.8			CloudWatc h.8

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Creat eLogMetri cFilterAn dAlarm Assicurat i che esistano un filtro metrico di log e un allarme per le modifiche alla configura zione di AWS Config		3.9		4.9			CloudWatc h.9

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Creat eLogMetri cFilterAn dAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativam ente alle modifiche apportate al gruppo di sicurezza		3.10		4,10			CloudWatc h.10

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Creat eLogMetri cFilterAn dAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativam ente alle modifiche apportate alle liste di controllo degli accessi alla rete (NACL)		3,11		4.11			CloudWatc h.11

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Creat eLogMetri cFilterAn dAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativam ente alle modifiche apportate ai gateway di rete		3,12		4,12			CloudWatc h.12

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Creat eLogMetri cFilterAn dAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativam ente alle modifiche apportate alle tabelle di routing		3.13		4,13			CloudWatc h.13

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Creat eLogMetri cFilterAn dAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativam ente alle modifiche apportate al VPC		3,14		4,14			CloudWatc h.14

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
AWS-DisablePublicAccessForSecurityGroup Assicurati che nessun gruppo di sicurezza consenta l'ingresso da 0.0.0.0/0 alla porta 22		4.1	EC2.5		EC2.13		EC2.13

Description	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
AWS-DisablePublicAccessForSecurityGroup Assicurati che nessun gruppo di sicurezza consenta l'ingresso da 0.0.0.0/0 alla porta 3389		4.2			EC2.14		EC2.14
ASR-ConfigureSNSTopicForStack	CloudFormation.1				CloudFormation.1		CloudFormation.1
ASR-CreateIAMSupportRole		1.20		1,17		1,17	IAM.18

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-DisablePublicIPAutoAssign Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici	EC2.15				EC2.15		EC2.15
ASR-EnableCloudTrailLogFileValidation	CloudTrail.4	2.2	CloudTrail.3	3.2			CloudTrail.4
ASR-EnableEncryptionForSNSTopic	SNS.1				SNS.1		SNS.1

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eDelivery StatusLog gingForSN STopic La registraz ione dello stato di consegna deve essere abilitata per i messaggi di notifica inviati a un argomento	SNS.2				SNS.2		SNS.2
ASR-Enabl eEncrypti onForSQSQ ueue	SQS.1				SQS.1		SQS.1

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-MakeRDSSnapshtPrivateL'istnea RDS deve essere privata	RDS.1		RDS.1				RDS.1
ASR-Block SSMDocumntPublicAccess I documenti SSM non devono essere pubblici	SSM.4				SSM.4		SSM.4

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eCloudFro ntDefault RootObjec t CloudFron t le distribuz ioni dovrebber o avere un oggetto root predefini to configura to	CloudFron t.1				CloudFron t.1		CloudFron t.1

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-SetCl oudFrontO riginDoma in CloudFron t le distribuz ioni non dovrebber o puntare a origini S3 inesisten ti	CloudFron t.12				CloudFron t.12		CloudFron t.12

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Remov eCodeBuil dPrivileg edMode CodeBuild gli ambienti di progetto dovrebber o avere una configura zione AWS di registraz ione	CodeBuild .5				CodeBuild .5		CodeBuild .5

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Termi nateEC2In stance Le istanze EC2 interrott e devono essere rimosse dopo un periodo di tempo specifica to	EC2.4				EC2.4		EC2.4

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eIMDSV2O Instance Le istanze EC2 devono utilizzare Instance Metadata Service versione 2 (IMDSv2)	EC2.8				EC2.8	5.6	EC2.8

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Revok eUnauthor izedInbou dRules I gruppi di sicurezza devono consentir e solo il traffico in entrata senza restrizio ni per le porte autorizza te	EC2.18				EC2.18		EC2.18

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Disab leUnrestr ictedAcce ssToHighR iskPorts I gruppi di sicurezza non dovrebber o consentir e l'accesso illimitato alle porte ad alto rischio	EC2.19				EC2.19		EC2.19

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Disab leTGWAutc AcceptSha redAttach ments Amazon EC2 Transit Gateways non dovrebbe accettare automatic amente richieste di allegati VPC	EC2.23				EC2.23		EC2.23

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl ePrivateR epository Scanning La scansione delle immagini deve essere configura ta nei repositor y privati ECR	ECR.1				ECR.1		ECR.1
ASR-Enabl eGuardDut y GuardDuty dovrebbe essere abilitato	GuardDuty .1		GuardDuty .1		GuardDuty .1		GuardDuty .1

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Confi gureS3Buc ketLoggin g La registraz ione degli accessi al server bucket S3 dovrebbe essere abilitata	S3.9				S3.9		S3.9
ASR-Enabl eBucketEv entNotifi cations I bucket S3 dovrebber o avere le notifiche degli eventi abilitate	S3.11				S3.11		S3.11

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-SetS3LifecyclePolicy I bucket S3 devono avere politiche relative al ciclo di vita configurate	S3.13				S3.13		S3.13
ASR-EnableAutoSecretRotation I segreti di Secrets Manager dovrebbero avere la rotazione automatica abilitata	SecretsManager.1				SecretsManager.1		SecretsManager.1

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-RemoveUnusedSecret Rimuovi i segreti inutilizzati di Secrets Manager	SecretsManager.3				SecretsManager.3		SecretsManager.3
ASR-UpdateSecretRotationPeriod I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni	SecretsManager.4				SecretsManager.4		SecretsManager.4

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eAPIGatew ayCacheDa taEncrypt ion I dati della cache dell'API REST di API Gateway devono essere crittogra fati quando sono inattivi					APIGatewa y.5		APIGatewa y.5

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-SetLo gGroupRet entionDay s CloudWatc h i gruppi di log devono essere conservat i per un periodo di tempo specifica to					CloudWatc h.16		CloudWatc h.16

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-AttachServiceVPCEndpoint Amazon EC2 deve essere configurato per utilizzare endpoint VPC creati per il servizio Amazon EC2	EC2.10				EC2.10		EC2.10
ASR-TagGuardDutyResource GuardDuty i filtri devono essere contrassegnati							GuardDuty.2

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-TagGu ardDutyRe source GuardDuty i rilevatori dovrebber o essere etichettati							GuardDuty .4
ASR-Attac hSSMPerm ssionsToE C2 Le istanze Amazon EC2 devono essere gestite da Systems Manager	SSM.1		SSM.3				SSM.1

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Confi gureLaunc hConfigNo PublicIPD ocument Le istanze Amazon EC2 avviate utilizzan do le configura zioni di avvio di gruppo Auto Scaling non devono avere indirizzi IP pubblici					AutoScali ng.5		AutoScali ng.5
ASR-Enabl eAPIGatew ayExecuti onLogs	APIGatewa y.1						APIGatewa y.1

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eMacie Amazon Macie deve essere abilitato	Macie.1				Macie.1		Macie.1
ASR-Enabl eAthenaWo rkGroupLo gging I gruppi di lavoro Athena devono avere la registraz ione abilitata	Athena.4						Athena.4

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enfor ceHTTPSF rALB Applicati on Load Balancer deve essere configura to per reindiriz zare tutte le richieste HTTP a HTTPS	ELB.1		ELB.1		ELB.1		ELB.1

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Limit ECSRootFilesystemAccess I contenitori ECS devono essere limitati all'accesso in sola lettura ai file system root	ECS.5				ECS.5		ECS.5

Description	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-EnableElastiCacheBackups ElastiCache I cluster (Redis OSS) dovrebbero avere i backup automatici abilitati	ElastiCache.1				ElastiCache.1		ElastiCache.1

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eElastiCa cheVersio nUpgrades ElastiCac he i cluster dovrebber o avere gli aggiornam enti automatic i delle versioni secondari e abilitati	ElastiCac he.2				ElastiCac he.2		ElastiCac he.2

Descripti on	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-Enabl eElastiCa cheReplic ationGrou pFailover ElastiCac he i gruppi di replica devono avere il failover automatic o abilitato	ElastiCac he.3				ElastiCac he.3		ElastiCac he.3

Description	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-ConfigureDynamoDBAutoScaling Le tabelle DynamoDB dovrebbero scalare automaticamente la capacità in base alla domanda	DynamoDB.1				DynamoDB.1		DynamoDB.1
ASR-TagDynamoDBTableResource Le tabelle DynamoDB devono essere contrassegnate							DynamoDB.5

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID di controllo di sicurezza
ASR-EnableDynamoDDeletionProtection Le tabelle DynamoDB devono avere la protezione dalle cancellazioni abilitata					DynamoDB.6		DynamoDB.6

Aggiungere nuove correzioni

Le correzioni possono essere aggiunte manualmente aggiornando i file di playbook appropriati o programmaticamente estendendo la soluzione tramite costrutti CDK, a seconda del flusso di lavoro preferito.

> **Note**
>
> Le istruzioni che seguono utilizzano le risorse installate dalla soluzione come punto di partenza. Per convenzione, la maggior parte dei nomi delle risorse delle soluzioni contiene ASR and/or SO0111 per facilitarne l'individuazione e l'identificazione.

Toolkit AI per correzioni personalizzate

Per accelerare i flussi di lavoro descritti in questa sezione, la soluzione fornisce l'AI Toolkit for Custom Remediations. Il toolkit raggruppa le migliori pratiche di correzione, i guardrail e i modelli di sviluppo di ASR sotto forma di istruzioni da fornire a un assistente AI nel tuo ambiente di sviluppo integrato (IDE). In questo contesto, l'assistente può aiutarti a creare runbook di ASR-compatible correzione, controllare runbook, ruoli IAM e costrutti CDK che seguono le convenzioni di denominazione e le fasi di integrazione documentate nelle sezioni seguenti, producendo correzioni personalizzate pronte per la produzione con meno iterazioni e maggiore sicurezza.

Il toolkit è opzionale e non modifica il modo in cui le correzioni vengono create o implementate; è un aiuto allo sviluppo che rende visibili le convenzioni e i vincoli della soluzione all'assistente AI. Rimani responsabile della revisione e del test di qualsiasi codice generato prima di distribuirlo.

Panoramica del flusso di lavoro manuale

La risposta automatica alla sicurezza sui runbook AWS deve seguire la seguente denominazione standard:

ASR- - - *<standard>* *<version>* *<control>*

Standard: l'abbreviazione dello standard di sicurezza. Questo deve corrispondere agli standard supportati dall'ASR. Deve essere uno tra «CIS», «AFSBP», «PCI», «NIST» o «SC».

Versione: la versione dello standard. Anche in questo caso, deve corrispondere alla versione supportata da ASR e alla versione nei dati di ricerca.

Controllo: l'ID di controllo del controllo da correggere. Questo deve corrispondere ai dati di ricerca.

1. Crea un runbook negli account dei membri.
2. Crea un ruolo IAM negli account dei membri.
3. (Facoltativo) Crea una regola di riparazione automatica nell'account amministratore.

Passaggio 1. Crea un runbook negli account dei membri

1. Accedi alla console di AWS Systems Manager e ottieni un esempio del JSON trovato.
2. Crea un runbook di automazione che corregga la scoperta. Nella scheda Owned by me, usa uno qualsiasi dei `ASR-` documenti nella scheda Documenti come punto di partenza.

3. Il runbook verrà eseguito da AWS Step Functions nell'account amministratore. Il runbook deve specificare il ruolo di correzione per essere passato quando si chiama il runbook.

Passaggio 2. Crea un ruolo IAM negli account dei membri

1. Accedi alla console di gestione delle identità e degli accessi di AWS.
2. Ottieni un esempio dai ruoli IAM SO0111 e crea un nuovo ruolo. Il nome del ruolo deve iniziare con SO0111-Remediate - - *<standard>* -*<version>*. *<control>* Ad esempio, se si aggiunge CIS v1.2.0 control 5.6, il ruolo deve essere. `SO0111-Remediate-CIS-1.2.0-5.6`
3. Utilizzando l'esempio, create un ruolo con ambito appropriato che consenta solo alle chiamate API necessarie di eseguire la correzione.

A questo punto, la correzione è attiva e disponibile per la correzione automatica dall'ASR Custom Action in AWS Security Hub.

Fase 3: (Facoltativo) Crea una regola di riparazione automatica nell'account amministratore

La correzione automatica (non «automatica») è l'esecuzione immediata della correzione non appena la scoperta viene ricevuta da AWS Security Hub. Valuta attentamente i rischi prima di utilizzare questa opzione.

1. Visualizza un esempio di regola per lo stesso standard di sicurezza in Amazon EventBridge. Lo standard di denominazione per le regole è`standard_control_*AutoTrigger*`.
2. Copia il modello di evento dall'esempio da utilizzare.
3. Cambia il `GeneratorId` valore in modo che corrisponda a quello `GeneratorId` nel tuo Finding JSON.
4. Salva e attiva la regola.

Panoramica del flusso di lavoro CDK

In sintesi, i seguenti file nel repository ASR verranno modificati o aggiunti. In questo esempio, una nuova correzione per ElastiCache.2 è stata aggiunta ai playbook SC e AFSBP.

> **Note**
>
> Tutte le nuove correzioni devono essere aggiunte al playbook SC, poiché consolida tutte le correzioni disponibili in ASR. Se intendi distribuire solo un set specifico di playbook (come AFSBP), puoi: (1) aggiungere la correzione solo ai playbook previsti oppure (2) aggiungere la correzione a tutti i playbook per cui esiste nel corrispondente Security Hub Standard, oltre al playbook SC. La seconda opzione è consigliata per la flessibilità.

In questo esempio, ElastiCache.2 è inclusa nei seguenti Security Hub Standards:

- AFSBP
- NIST.800-53.r5 SI-2
- NIST.800-53.r5 SI-2(2)
- NIST.800-53.r5 SI-2(4)
- NIST.800-53.r5 SI-2(5)
- PCI DSS v4.0. 1/63.3.3

Poiché, per impostazione predefinita, ASR implementa solo i playbook per AFSBP e NIST.800-53 aggiungeremo questa nuova correzione a tali playbook oltre a SC.

Modifica

- source/lib/remediation-runbook-stack.ts
- source/playbooks//[nome standard] _remediations.ts AFSBP/lib
- source/playbooksNIST80053/lib/control/_runbooks-construct.ts
- source/playbooks//[nome standard] _remediations.ts NIST80053/lib
- source/playbooksSC/lib/control/_runbooks-construct.ts
- source/playbooks/SC/lib/sc_bonificazioni.ts
- source/test/regex_registry.ts

Add

- source/playbooks/SC/ssmdocs/SC_ElastiCache.2.ts

- source/playbooks/SC/ssmdocs/descriptions/ElastiCache.2.md
- source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml

> **Note**
>
> Il nome scelto per il runbook può essere qualsiasi stringa, purché sia coerente con il resto delle modifiche apportate.

- source/playbooks/NIST80053/ssmdocs/NIST80053_ElastiCache.2.ts
- source/playbooks/AFSBP/ssmdocs/AFSBP_ElastiCache.2.yaml

Fasi di sviluppo

1. Crea il Remediation Runbook.
2. Crea i Control Runbook.
3. Integra ogni Control Runbook con un Playbook.
4. Crea il Remediation IAM Role e integra il Remediation Runbook
5. Aggiorna i test unitari

Fase 1: Creare il Remediation Runbook

Questo è il documento SSM utilizzato per rimediare alle risorse. Deve includere il `AutomationAssumeRole` parametro, che è il ruolo IAM con le autorizzazioni per eseguire la correzione. Visualizza il file esistente `source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml` come riferimento durante la creazione di nuovi runbook di riparazione.

Tutti i nuovi runbook devono essere aggiunti alla directory. `source/remediation_runbooks/`

Passaggio 2: creare i Control Runbook

Un runbook di controllo è un runbook specifico per il playbook che analizza i dati di ricerca dello standard specificato ed esegue il Remediation Runbook appropriato. Poiché stiamo aggiungendo la ElastiCache.2 correzione ai playbook SC, AFSBP e NIST80053, dobbiamo creare un nuovo runbook di controllo per ciascuno. Vengono creati i seguenti file:

- source/playbooks/SC/ssmdocs/SC_ElastiCache.2.ts
- source/playbooks/NIST80053/ssmdocs/NIST80053_ElastiCache.2.ts
- source/playbooks/AFSBP/ssmdocs/AFSBP_ElastiCache.2.yaml

Example

La denominazione di questi file è importante e deve seguire il formato <PLAYBOOK_NAME>_< >CONTROL.ID. ts/yaml

Alcuni playbook in ASR supportano i runbook di controllo IaC in TypeScript, mentre altri devono essere scritti in YAML grezzo. Fai riferimento alle correzioni esistenti nel rispettivo playbook come esempi. In questo esempio, tratteremo il playbook SC, che utilizza IaC.

Nel playbook SC, il nuovo runbook di controllo dovrebbe esportare una classe che si estende ControlRunbookDocument e corrisponde al nome del runbook di riparazione. Dai un'occhiata all'esempio seguente:

```
export class EnableElastiCacheVersionUpgrades extends ControlRunbookDocument {
  constructor(scope: Construct, id: string, props: ControlRunbookProps) {
    super(scope, id, {
      ...props,
      securityControlId: 'ElastiCache.2',
      remediationName: 'EnableElastiCacheVersionUpgrades',
      scope: RemediationScope.REGIONAL,
      resourceIdRegex: <Regex>,
      resourceIdName: 'ClusterId',
      updateDescription: new StringFormat('Automatic minor version upgrades enabled for
 cluster %s.', [
        StringVariable.of(`ParseInput.ClusterId`),
      ]),
    });
  }
}
```

- `securityControlId`è l'ID di controllo per la correzione che stai aggiungendo, come definito nella vista dei controlli consolidati in Security Hub.
- `remediationName`è il nome che hai scelto per il tuo runbook di riparazione.
- `scope`è l'ambito della risorsa da correggere, indicando se esiste a livello globale o in una regione specifica.

- `resourceIdRegex`è l'espressione regolare utilizzata per acquisire l'ID della risorsa che desideri passare al runbook di riparazione come parametro. È necessario acquisire un solo gruppo, tutti gli altri gruppi non devono essere acquisiti. Se desideri passare l'intero ARN, ometti questo campo.
- `resourceIdName`è il nome che desideri impostare per l'ID della risorsa acquisita utilizzando`resourceIdRegex`, dovrebbe corrispondere al nome del parametro ID della risorsa nel runbook di riparazione.
- `updateDescription`è la stringa che desideri assegnare alla sezione «note» del risultato in Security Hub una volta completata la correzione.

È inoltre necessario esportare una funzione chiamata `createControlRunbook` che restituisce una nuova istanza della classe. Perché ElastiCache.2, questo assomiglia a:

```
export function createControlRunbook(scope: Construct, id: string, props:
 PlaybookProps): ControlRunbookDocument {
  return new EnableElastiCacheVersionUpgrades(scope, id, { ...props, controlId:
 'ElastiCache.2' });
}
```

`controlId`dov'è l'ID di controllo definito nello standard di sicurezza associato al playbook in base al quale si opera.

Se il controllo Security Hub contiene parametri da passare al runbook di riparazione, è possibile passarli aggiungendo delle sostituzioni ai seguenti metodi: -`getExtraSteps`: definisce i valori predefiniti per ogni parametro implementato per il controllo in Security Hub

> **Note**
>
> A ogni parametro di Security Hub deve essere assegnato un valore predefinito

- `getInputParamsStepOutput`: definisce gli output per la GetInputParams fase del runbook di controllo
- Ogni uscita ha un `nameoutputType`, e. `selector` `selector`Dovrebbe essere lo stesso selettore utilizzato nell'override del `getExtraSteps` metodo.
- `getRemediationParams`: definisce i parametri passati al runbook di riparazione, recuperati dagli output dello step. GetInputParams

Per visualizzare un esempio, accedi al file. `source/playbooks/SC/ssmdocs/SC_DynamoDB.1.ts`

Passaggio 3: integra ogni Control Runbook con un Playbook

Per ogni runbook di controllo creato nel passaggio precedente, è ora necessario integrarlo con le definizioni dell'infrastruttura nel playbook associato. Segui i passaggi seguenti per ogni runbook di controllo.

> **Important**
>
> Se hai creato il runbook di controllo usando YAML raw anziché typescript IaC, passa alla sezione successiva.

In */<playbook_name>/*`control_runbooks-construct.ts` Importa il tuo file di controllo runbook appena creato, ad esempio:

```
import * as elasticache_2 from '../ssmdocs/SC_ElastiCache.2';
```

Quindi, vai all'array per

```
const controlRunbooksRecord: Record<string, any>
```

E aggiungi una nuova voce che associa l'ID di controllo (specifico del playbook) al `createControlRunbook` metodo che hai creato:

```
'ElastiCache.2': elasticache_2.createControlRunbook,
```

Aggiungi l'ID di controllo specifico di playbook all'elenco delle correzioni nel modo seguente: *<playbook_name>*`\_remediations.ts`

```
{ control: 'ElastiCache.2', versionAdded: '2.3.0' },
```

Il `versionAdded` campo deve essere la versione più recente della soluzione. Se l'aggiunta della correzione viola il limite di dimensione del modello, aumenta il. `versionAdded` Puoi modificare il numero di correzioni incluse in ogni stack di membri del playbook in. `solution_env.sh`

Fase 4: Creare il Remediation IAM Role & Integrate Remediation Runbook

Ogni correzione ha il proprio ruolo IAM con le autorizzazioni personalizzate necessarie per eseguire il runbook di correzione. Inoltre, è necessario richiamare il `RunbookFactory.createRemediationRunbook` metodo per aggiungere il runbook di riparazione creato nel passaggio 1 ai modelli della soluzione. CloudFormation

In`remediation-runbook-stack.ts`, ogni correzione ha il proprio blocco di codice nella classe. `RemediationRunbookStack` Il seguente blocco di codice mostra la creazione di un nuovo ruolo IAM e l'integrazione del runbook di riparazione per la correzione: ElastiCache.2

```
    //-----------------------
    // EnableElastiCacheVersionUpgrades
    //
    {
      const remediationName = 'EnableElastiCacheVersionUpgrades'; // should match the
 name of your remediation runbook
      const inlinePolicy = new Policy(props.roleStack, `ASR-Remediation-Policy-
${remediationName}`);

      const remediationPolicy = new PolicyStatement();
      remediationPolicy.addActions('elasticache:ModifyCacheCluster');
      remediationPolicy.effect = Effect.ALLOW;
      remediationPolicy.addResources(`arn:${this.partition}:elasticache:*:
${this.account}:cluster:*`);
      inlinePolicy.addStatements(remediationPolicy);

      new SsmRole(props.roleStack, 'RemediationRole ' + remediationName, { // creates
 the remediation IAM role
        solutionId: props.solutionId,
        ssmDocName: remediationName,
        remediationPolicy: inlinePolicy,
        remediationRoleName: `${remediationRoleNameBase}${remediationName}`,
      });

      RunbookFactory.createRemediationRunbook(this, 'ASR ' + remediationName, { // adds
 the remediation runbook to the solution's cloudformation templates
        ssmDocName: remediationName,
        ssmDocPath: ssmdocs,
        ssmDocFileName: `${remediationName}.yaml`,
        scriptPath: `${ssmdocs}/scripts`,
        solutionVersion: props.solutionVersion,
        solutionDistBucket: props.solutionDistBucket,
```

```
        solutionId: props.solutionId,
        namespace: namespace,
      });
    }
```

Fase 5: Aggiornamento dei test unitari

Consigliamo di aggiornare ed eseguire gli unit test dopo aver aggiunto una nuova correzione.

Innanzitutto, è necessario aggiungere qualsiasi nuova espressione regolare (che non sia già stata aggiunta) nel `source/test/regex_registry.ts` file. Questo file impone il test per ogni nuova espressione regolare inclusa nei runbook della soluzione. Date un'occhiata alla `addElastiCacheClusterTestCases` funzione come esempio, che viene utilizzata per testare le espressioni regolari utilizzate nelle ElastiCache correzioni.

Infine, dovrai aggiornare le istantanee per ogni stack. Le istantanee sono definizioni di CloudFormation modelli controllate dalla versione che vengono utilizzate per tenere traccia delle modifiche apportate all'infrastruttura di ASR. Aggiornate i file delle istantanee eseguendo il seguente comando dalla directory: `deployment`

```
./run-unit-tests.sh update
```

Ora sei pronto per implementare la tua nuova correzione! Vai alla sezione Build and Deploy di seguito per istruzioni su come creare e distribuire la soluzione con le nuove modifiche.

Aggiungere un nuovo playbook

Scarica i playbook della soluzione Automated Security Response on AWS e il codice sorgente di distribuzione dal repository. GitHub

Le CloudFormation risorse AWS sono create dai componenti AWS CDK e contengono il codice del modello di playbook che puoi utilizzare per creare e configurare nuovi playbook. Per ulteriori informazioni sulla configurazione del progetto e sulla personalizzazione dei playbook, consulta il file in. README.md GitHub

AWS Systems Manager Parameter Store

Automated Security Response on AWS utilizza AWS Systems Manager Parameter Store per l'archiviazione dei dati operativi. I seguenti parametri sono memorizzati in Parameter Store:

Nome	Valore	Utilizzo
`/Solutions/SO0111/CMK_REMEDIATION_ARN`	Chiave AWS KMS che crittograferà i dati per le correzioni FSBP	Crittografia dei dati dei clienti, come i CloudTrail log, come parte delle correzioni
`/Solutions/SO0111/CMK_ARN`	Chiave AWS KMS che ASR utilizzerà per crittografare i dati	Crittografia dei dati della soluzione
`/Solutions/SO0111/SNS_Topic_ARN`	ARN dell'argomento Amazon SNS relativo alla soluzione	Notifica degli eventi di riparazione
`/Solutions/SO0111/SNS_Topic_Config.1`	Argomento SNS per gli aggiornamenti di AWS Config	Config.1 riparazione
`/Solutions/SO0111/version`	Versione della soluzione	
`/Solutions/SO0111/`*`<security standard long name>`*`/`*`<version>`* /status	`enabled`	Indica se lo standard è attivo nella soluzione. Uno standard può essere disabilitato per la correzione automatica modificandolo in `disabled`
`/Solutions/SO0111` // shortname *`<security standard long name>`*	`String`	Nome abbreviato dello standard di sicurezza. Ad esempio:`CIS`,`AFSBP`, `PCI`
`/Solutions/SO0111//`*`<security standard long name><version>`* */`*`<control>`* /rimappa	`String`	Quando un controllo utilizza la stessa correzione di un altro, questi parametri eseguono la rimappatura
`/ASR/Filters/AccountFilterMode`	Includi, escludi o disabilitato	Controlla il comportamento di filtraggio degli ID dell'account per correzioni completamente automatiche

Nome	Valore	Utilizzo
`/ASR/Filters/AccountFilters`	Comma-delimited elenco degli ID degli account AWS	Elenco degli ID degli account AWS per i quali la soluzione deve filtrare le correzioni automatiche.
`/ASR/Filters/OUFilterMode`	Includi, escludi o disabilita	Controlla il comportamento di filtraggio delle unità organizzative (OU) per correzioni completamente automatizzate
`/ASR/Filters/OUFilters`	Comma-delimited elenco degli ID delle unità organizzative	Elenco delle unità organizzative per le quali la soluzione deve filtrare le correzioni automatiche.
`/ASR/Filters/TagFilterMode`	Includi, escludi o disabilita	Controlla il comportamento di filtraggio dei Resource Tag per correzioni completamente automatiche
`/ASR/Filters/TagFilters`	Comma-delimited elenco delle chiavi dei Resource Tag	Elenco delle chiavi dei tag delle risorse per le quali la soluzione deve filtrare le correzioni automatiche.

Argomento Amazon SNS - Progresso della riparazione

La risposta di sicurezza automatica su AWS crea un argomento Amazon SNS, SO0111-ASR _Topic. Questo argomento viene utilizzato per pubblicare aggiornamenti sull'avanzamento della correzione. Di seguito sono riportate le tre possibili notifiche inviate a questo argomento.

```
Remediation queued for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
Remediation failed for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
[.replaceable]`<control_ID>` remediation was successfully invoke via AWS Systems
 Manager in account [.replaceable]`<account_ID>`
```

Questo è il messaggio di completamento. Indica che la correzione è stata completata senza errori; tuttavia, il test definitivo per una corretta riparazione è la convalida manuale del controllo di AWS Config. and/or

Filtraggio di un abbonamento a un argomento SNS

Politiche di filtro degli abbonamenti Amazon SNS:

1. Passa alla sottoscrizione dell'argomento SNS.
2. In Politica di filtro dell'abbonamento, scegli Modifica.
3. Espandi «Politica di filtro degli abbonamenti» e attiva l'opzione «Politica di filtro degli abbonamenti» per abilitare i filtri.
4. Scegli l'ambito «Corpo del messaggio».
5. Aggiungi la tua policy all'editor JSON.
6. Salva le modifiche.

Politiche di esempio:

Filtra per account

```
{
"finding": {
"account": [
"111111111111",
"222222222222"
]
}
}
```

Filtra per gli errori

```
{
"severity": ["ERROR"]
}
```

Filtra per controlli

```
{
"finding": {
"standard_control": ["S3.9","S3.6"]
}
}
```

Argomento Amazon SNS: allarmi CloudWatch

Questa soluzione crea un argomento Amazon SNS,. `S00111-ASR_Alarm_Topic` Questo argomento viene utilizzato per pubblicare avvisi di allarme.

I dettagli di tutti gli allarmi che entrano nello stato ALARM verranno inviati a questo argomento.

Avvia Runbook on Config Findings

Questa soluzione può avviare runbook in base a risultati personalizzati di AWS Config. Per farlo, completa le seguenti fasi.

1. Trova il nome della regola AWS Config a cui desideri correggere. Questo può essere trovato in AWS Config o nella constatazione generata da Security Hub per questa regola.
2. Accedi a AWS Systems Manager Parameter Store e seleziona Create Parameter.
3. Il nome della regola deve essere `/Solutions/S00111/` [.replaceable] `Rule name from Step 1`
4. Il valore deve essere formattato come segue:

```
{
"RunbookName":"Name of SSM runbook",
"RunbookRole": "Role that Orchestrator will assume"
}
```

1. RunbookName è un campo obbligatorio. Specifica il runbook che viene eseguito quando si corregge questa regola di AWS Config. RunbookRole è il ruolo che l'orchestrator assume durante l'esecuzione di questa correzione. Non è un campo obbligatorio e, se omesso, l'orchestrator utilizza per impostazione predefinita il ruolo di membro dell'account.
2. Una volta completata questa operazione, puoi correggere la regola di AWS Config utilizzando l'azione personalizzata «Remediate with ASR» disponibile nel Security Hub.

Interfaccia utente Web

L'interfaccia utente Web della soluzione consente agli utenti di correggere i risultati di AWS Security Hub con un clic, visualizzare e scaricare le correzioni precedenti e delegare l'accesso alla soluzione.

L'interfaccia utente Web non è richiesta per utilizzare la soluzione; in alternativa è possibile configurare correzioni completamente automatiche per evitare la necessità di eseguire manualmente, o sfruttare la console CSPM di AWS Security Hub per avviare le correzioni utilizzando l'azione personalizzata Remediate with ASR.

> **Note**
>
> È necessario impostare il `ShouldDeployWebUI` parametro su «yes» quando si distribuisce lo stack di amministrazione per utilizzare l'interfaccia utente Web della soluzione.

Come funziona

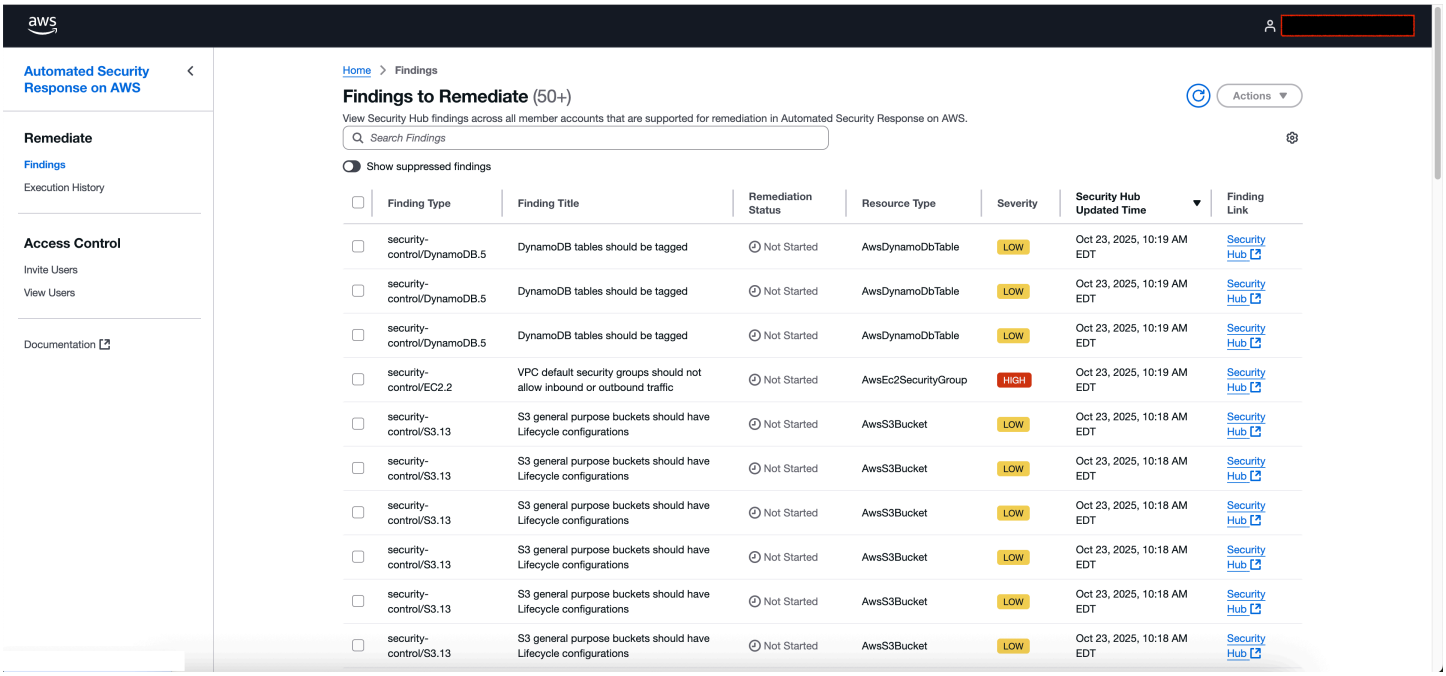
L'interfaccia utente Web della soluzione è un'applicazione Single-Page Web ospitata nel tuo account da Amazon S3 e distribuita da Amazon. CloudFront La soluzione implementa anche un'API REST utilizzando API Gateway per supportare le operazioni nell'interfaccia utente Web.

Quando lo stack di amministrazione viene distribuito, le funzioni Lambda della soluzione iniziano a caricare in DynamoDB tutti i risultati di AWS Security Hub supportati dalla soluzione presenti nel tuo account di amministratore. Una volta completato, i risultati presentati nell'interfaccia utente Web vengono mantenuti sincronizzati con Security Hub quasi in tempo reale grazie alle EventBridge regole implementate dalla soluzione.

Ogni settimana, la soluzione attiva le sue funzioni Lambda per aggiornare la tabella DynamoDB che memorizza i risultati di AWS Security Hub visualizzati nell'interfaccia utente Web. È progettato

per ripulire i dati obsoleti e mantenere aggiornate le tabelle DynamoDB. Se desideri configurare questa linea di base in modo che venga eseguita più o meno spesso, modifica la EventBridge Regola denominata che `SO0111-ASR-SynchronizationFindingsLambdaWeeklyRule` si trova nel tuo account di amministratore nella stessa regione in cui hai implementato la soluzione.

Esegui le correzioni direttamente nell'interfaccia utente Web



Nella pagina dei risultati, gli utenti amministratori o amministratori delegati possono visualizzare tutti i risultati di AWS Security Hub supportati dalla soluzione per la correzione. Ciò include i risultati relativi agli account membri di Security Hub integrati con l'account principale di Security Hub. Se la soluzione è implementata anche nell'area di aggregazione, verranno visualizzati anche i risultati in qualsiasi regione integrata. Per visualizzare l'elenco dei risultati supportati dalla soluzione, consulta la sezione dei playbook. ???

Gli utenti di Account Operator saranno in grado di visualizzare solo i risultati provenienti dagli account AWS a cui hanno accesso come definito nel loro invito. Inoltre, saranno in grado di eseguire correzioni solo per le risorse negli account a cui sono associati.

Per eseguire le correzioni, seleziona un numero qualsiasi di elementi nella tabella e scegli Azioni > Ripara. Puoi anche eliminare i risultati scegliendo Azioni > Sopprimi, che nasconde i risultati selezionati dalla vista predefinita. È possibile visualizzare i risultati soppressi in qualsiasi momento selezionando l'opzione Mostra risultati soppressi.

Una volta avviata la correzione di un risultato, è possibile scegliere la colonna Stato della riparazione mentre la correzione è in corso `In Progress` oppure accedere direttamente `Failed` alla correzione nella pagina Cronologia delle esecuzioni.

Filtra i risultati e le correzioni disponibili

In entrambe le pagine Risultati e Cronologia delle esecuzioni, puoi filtrare i dati visualizzati nella tabella in base a una qualsiasi delle colonne presenti in ciascuna rispettiva tabella.

Ad esempio, nella pagina Risultati, puoi filtrare in base al tipo di ricerca per cercare tipi specifici di risultati di AWS Security Hub (come Lambda.1 o Athena.4) scegliendo la barra di ricerca e selezionando Tipo di ricerca.

> **Note**
>
> I valori che vengono compilati automaticamente nella barra di ricerca non rappresentano un elenco completo dei dati disponibili. I valori suggeriti per ogni criterio di ricerca rappresentano solo i dati attualmente recuperati e visualizzati nell'interfaccia utente.

Puoi anche combinare più attributi in un'unica ricerca. Ad esempio, puoi applicare sia il tipo di ricerca che l'ID della risorsa nella ricerca per eseguire una `AND` query logica. Inoltre, è possibile applicare più criteri di filtro uguali per eseguire una `OR` ricerca logica, ad esempio Finding Type = Lambda.1 e Finding Type = Athena.4. Gli stessi principi si applicano alla pagina Cronologia delle esecuzioni

&Autorizzazione all'autenticazione nell'interfaccia utente Web

L'interfaccia utente Web della soluzione è protetta dall'autenticazione fornita da Amazon Cognito. Quando la soluzione viene implementata, un pool di utenti Cognito, un client per app Cognito e un dominio del pool di utenti Cognito vengono forniti e configurati insieme all'interfaccia utente Web. All'indirizzo e-mail fornito come parametro allo stack di amministrazione vengono assegnate credenziali temporanee e viene concesso l'accesso di amministratore all'interfaccia utente Web.

Esistono tre tipi di autorizzazione che definiscono l'accesso di un utente all'interfaccia utente Web:

Tipo di autorizzazione	Livello di accesso	Caso d'uso
Admin	Controllo completo nell'interfaccia utente Web; può visualizzare tutti i risultati e le correzioni, eseguire eventuali correzioni e invite/view qualsiasi utente.	Assegnato solo all'utente che ha implementato lo stack di amministrazione quando fornisce il proprio indirizzo email durante la distribuzione. CloudFormation
Amministratore delegato	Controllo elevato nell'interfaccia utente Web; può visualizzare tutti i risultati e le correzioni, eseguire eventuali correzioni e gli utenti dell'Account Operator. invite/view Non è possibile invitare o visualizzare amministratori e amministratori delegati nell'interfaccia utente Web.	L'utente amministratore può delegare l'accesso alla soluzione invitando gli utenti amministratori delegati, che saranno in grado di eseguire e gestire eventuali correzioni.
Operatore dell'account	Controllo limitato nell'interfaccia utente Web; limitato alla visualizzazione e alla correzione dei risultati solo negli account a cui sono associati su invito. Impossibile invitare o visualizzare utenti aggiuntivi.	Day-to-day utenti che dovrebbero avere un accesso limitato per eseguire le correzioni in un sottoinsieme di account integrati. Gli amministratori o gli amministratori delegati hanno la responsabilità di invitare questi utenti e definirne l'ambito.

Tutti gli utenti devono essere invitati da un amministratore o da un amministratore delegato prima di poter accedere all'interfaccia utente Web. Per invitare altri utenti, un amministratore o un amministratore delegato può inserire il proprio indirizzo e-mail e il livello di autorizzazione nella pagina Invita utenti dell'interfaccia utente Web.

Gli amministratori e gli amministratori delegati possono anche visualizzare, gestire ed eliminare gli utenti esistenti. Per visualizzare un elenco di tutti gli utenti, vai alla pagina Visualizza utenti.

Per gestire un utente esistente, seleziona l'utente dalla tabella e scegli Gestisci utente. È quindi possibile eliminare l'utente scegliendo Elimina utente. Se l'utente è un Account Operator, puoi modificare l'elenco degli ID degli account AWS a cui ha accesso nel contesto della soluzione. La modifica del tipo di autorizzazione per un utente esistente non è attualmente supportata.

Gli amministratori delegati possono visualizzare e gestire solo gli utenti di Account Operator.

Integrazione con sistemi esterni IdPs

Puoi personalizzare il meccanismo di autenticazione fornito dalla soluzione per consentire agli utenti di accedere utilizzando il tuo provider di identità OIDC o SAML, come Okta o Microsoft Entra ID. I seguenti passaggi per l'integrazione con l'esterno IdPs richiedono l'accesso all'account AWS in cui è distribuito lo stack di amministrazione.

> **Important**
>
> Gli utenti devono comunque essere invitati prima di accedere utilizzando qualsiasi IdP esterno configurato per funzionare con la soluzione. Inoltre, l'indirizzo e-mail collegato al loro profilo IdP deve corrispondere all'indirizzo e-mail fornito nell'invito.

Passaggio 1: individua il pool di utenti della soluzione

Nella console Amazon Cognito, individua il pool di utenti della soluzione denominato SO0111-ASR-UserPool.

Scegli il nome del pool di utenti SO0111-ASR-UserPool da portare alla pagina di panoramica. Da lì, scegli Provider social ed esterni dalla barra di navigazione.

Passaggio 2: aggiungi il tuo provider di identità

Nella pagina dei provider social ed esterni, scegli il pulsante Aggiungi provider di identità in alto a destra.

Seleziona OIDC o SAML, a seconda del tuo provider di identità.

Dopo aver selezionato il tipo di provider, ti verrà richiesto di inserire le informazioni sul tuo provider di identità.

Compila i seguenti campi per i provider SAML:

1. Nome del provider: un nome descrittivo per il tuo provider
2. IdP-initiated Accesso SAML: seleziona `Require SP-initiated SAML assertions - Recommended`
3. Fonte del documento con metadati: Seleziona `Upload metadata document`
4. Documento di metadati: carica il documento di metadati SAML fornito dal tuo IdP.
5. In Mappa gli attributi tra il tuo provider SAML e il tuo pool di utenti, scegli Aggiungi un altro attributo. Per l'attributo del pool di utenti, seleziona `email` dal menu a discesa. Per l'attributo SAML, inserisci il nome completo dell'attributo in cui l'indirizzo email dell'utente è memorizzato nel tuo provider di identità SAML. Ad esempio, `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`.
6. Scegli Aggiungi provider di identità per salvare le modifiche.

Compila i seguenti campi per i provider OIDC:

1. Nome del fornitore: un nome descrittivo per il tuo provider
2. ID cliente: inserisci l'ID cliente fornito dal tuo provider di identità OpenID Connect.
3. Segreto del cliente: Inserisci il segreto del cliente fornito dal provider di identità OpenID Connect.
4. Ambiti autorizzati: Inserisci `openid profile email`
5. Metodo di richiesta degli attributi: seleziona `GET` o `POST` in base alla configurazione del tuo provider di identità.
6. Metodo di configurazione: seleziona `Auto fill through issuer URL` e inserisci l'URL dell'emittente del tuo provider OIDC. In alternativa, inserisci i valori manualmente.
7. In Mappa gli attributi tra il tuo provider OpenID Connect e il tuo pool di utenti, scegli Aggiungi un altro attributo. Per l'attributo del pool di utenti, seleziona `email` dal menu a discesa. Per l'attributo OpenID Connect, inserisci il nome completo dell'attributo in cui l'indirizzo email dell'utente è memorizzato nel tuo provider di identità OIDC. Ad esempio, `email`.
8. Scegli Aggiungi provider di identità per salvare le modifiche.

> **Important**
>
> È necessario aggiungere una mappatura degli attributi per l'attributo del pool di `email` utenti, anche se lo è anche `email` il nome dell'attributo del provider di identità.

Passaggio 3: aggiungi il tuo provider all'App Client della soluzione

Vai alla pagina App Clients e seleziona il nome del client SO0111-ASR-WebUI-UserPoolClient.

Scegli la scheda Pagine di accesso e in Configurazione delle pagine di accesso gestite scegli Modifica.

Nel campo Provider di identità, aggiungi il provider di identità che hai creato nel passaggio precedente. Seleziona Salva modifiche.

Passaggio 4: configura il tuo provider di identità

Per consentire al provider di identità di reindirizzare all'interfaccia utente Web della soluzione dopo l'accesso, è necessario inserire nell'elenco i seguenti URL nella configurazione IdP.

A seconda del tipo di provider, inserisci nella lista consentita uno dei seguenti URL di callback:

1. URL di callback SAML: .auth. https://so0111-asr- *<your-aws-account-id>* *<aws-region>*.amazoncognito. com/saml2risposta /id
2. URL di richiamata OIDC: .auth. https://so0111-asr- *<your-aws-account-id>* *<aws-region>*.amazon cognito. com/oauth2risposta /id

È necessario sostituirlo `<your-aws-account-id>` con l'ID dell'account AWS in cui è stato distribuito lo stack di amministrazione e `<aws-region>` con la regione in cui è stato distribuito lo stack di amministrazione.

Passaggio 5: verifica la tua integrazione

Vai alla pagina di accesso all'interfaccia utente Web. Verifica che il tuo provider di identità personalizzato sia visibile nella pagina di accesso.

Per testare l'integrazione, invita un nuovo utente utilizzando la pagina Invita utenti. Quindi, assicurati che l'utente possa autenticarsi scegliendo il tuo provider di identità personalizzato nella pagina di accesso dell'interfaccia utente Web.

Il profilo dell'utente nel tuo IdP personalizzato deve essere collegato allo stesso indirizzo email fornito nell'invito. In altre parole, l'indirizzo email indicato nelle richieste del provider deve corrispondere all'invito.

Riferimento

Questa sezione include informazioni su una funzionalità opzionale per la raccolta dei dati, riferimenti alle risorse correlate e un elenco di costruttori che hanno contribuito a questa soluzione.

Raccolta dei dati

Questa soluzione invia metriche operative ad AWS (i «Dati») sull'uso di questa soluzione. Utilizziamo questi dati per capire meglio come i clienti utilizzano questa soluzione e i servizi e i prodotti correlati. La raccolta di questi dati da parte di AWS è soggetta all'Informativa sulla privacy di AWS.

Risorse correlate

- Risposta e riparazione automatiche con AWS Security Hub
- Benchmark CIS Amazon Web Services Foundations, versione 1.2.0
- Standard AWS Foundational Security Best Practices
- Payment Card Industry Data Security Standard (PCI DSS)
- Istituto nazionale di standard e tecnologia (NIST) SP 800-53 Rev. 5

Collaboratori

Le seguenti persone hanno contribuito a questo documento:

- Mike O'Brien
- Nikhil Reddy
- Chandini Penmetsa
- Chaitanya Deolankar
- Max Granat
- Tim Mekari
- Aaron Schütter
- Andrew Yankowsky
- Josh Moss
- Ryan Garay

- Thiemo Belmega
- Mikhailo Markhain
- Manish Jangid
- Andrew Stephen
- Pietro DeVries
- Mukta Dadariya
- Emanuel George
- Harika Kondakindi
- Narmeen Ali

Revisioni

Data di pubblicazione: agosto 2020 (ultimo aggiornamento: gennaio 2025)

Visita Changelog.md nel nostro GitHub repository per tenere traccia dei miglioramenti e delle correzioni specifici della versione.

Note

I clienti sono responsabili della propria valutazione indipendente delle informazioni contenute nel presente documento. Questo documento: (a) è solo a scopo informativo, (b) rappresenta le attuali offerte e pratiche di prodotti AWS, che sono soggette a modifiche senza preavviso, e (c) non crea alcun impegno o garanzia da parte di AWS e delle sue affiliate, fornitori o licenzianti. I prodotti o i servizi AWS sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite. Le responsabilità e gli obblighi di AWS nei confronti dei propri clienti sono controllati da accordi AWS e questo documento non fa parte né modifica alcun accordo tra AWS e i suoi clienti.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.