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 riparazione predefinite in AWS Security Hub

Data di pubblicazione: agosto 2020 (ultimo aggiornamento: dicembre 2024)

Questa guida all'implementazione fornisce una panoramica della AWS soluzione Automated Security Response on, della sua architettura e dei suoi componenti di riferimento, considerazioni per la pianificazione della distribuzione, i passaggi di configurazione per la distribuzione della AWS soluzione Automated Security Response on su Amazon Web Services (AWS) Cloud.

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

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

La continua evoluzione della sicurezza richiede misure proattive per proteggere i dati, il che può rendere difficile, costosa e dispendiosa in termini di tempo la reazione dei team di sicurezza. La AWS soluzione Automated Security Response on consente di reagire rapidamente per risolvere i problemi di sicurezza fornendo risposte e azioni correttive predefinite basate sugli standard di conformità del settore e sulle migliori pratiche.

Automated Security Response on AWS è una AWS soluzione che migliora la sicurezza e aiuta ad allineare i carichi di lavoro alle best practice del pilastro Well-Architected Security (0). AWS Security HubSEC1 Questa soluzione consente AWS Security Hub ai clienti di risolvere più facilmente i problemi di sicurezza comuni e migliorare il loro livello di sicurezza in. AWS

È possibile selezionare playbook specifici da distribuire nell'account principale di Security Hub. Ogni playbook contiene le azioni personalizzate necessarie, i ruoli di Identity and Access Management (IAM), EventBridge le regole Amazon, i documenti di automazione di AWS Systems Manager e AWS Lambdale funzioni AWS Step Functionsnecessarie per avviare un flusso di lavoro di riparazione all'interno di un singolo AWS account o tra più account. Le riparazioni funzionano dal menu Azioni AWS Security Hub e consentono agli utenti autorizzati di correggere un problema in tutti gli account AWS Security Hub gestiti con un'unica azione. Ad esempio, puoi applicare i consigli del Center for Internet Security (CIS) AWS Foundations Benchmark, uno standard di conformità per la protezione delle AWS risorse, per garantire che le password scadano entro 90 giorni e applicare la crittografia dei registri degli eventi archiviati. AWS

> **Note**
>
> La riparazione è destinata a situazioni emergenti che richiedono un'azione immediata. Questa soluzione apporta modifiche ai risultati della correzione solo se avviata dall'utente tramite la console di AWS Security Hub gestione o quando la riparazione automatica è stata abilitata utilizzando la EventBridge regola di Amazon per un controllo specifico. Per annullare queste modifiche, devi riportare manualmente le risorse allo stato originale.
> Quando ripristini le AWS risorse 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'AWS CloudFormation utente.

Automated Security Response on AWS include il playbook delle correzioni per gli standard di sicurezza definiti come parte di quanto segue:

- Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0
- CISAWSFondamenti di Benchmark v1.4.0
- CISAWSFondamenti di Benchmark v3.0.0
- AWSMigliori pratiche di sicurezza di base () v.1.0.0 FSBP

- 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 di risultati di controllo consolidati di AWS Security Hub. Per ulteriori informazioni, consulta Playbook.

Questa guida all'implementazione illustra le considerazioni architettoniche e le fasi di configurazione per l'implementazione dell'Automated Security Response su una AWS soluzione nel cloud. AWS Include collegamenti a AWS CloudFormationmodelli che avviano, configurano ed eseguono i servizi di AWS elaborazione, rete, storage e altri servizi necessari per implementare questa soluzioneAWS, utilizzando le AWS migliori pratiche per la sicurezza e la disponibilità.

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

Funzionalità e vantaggi

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

Correggi automaticamente i risultati per controlli specifici

Attiva EventBridge le regole Amazon per i controlli per correggere automaticamente i risultati relativi a quel controllo subito dopo la loro comparsa in AWS Security Hub.

Gestisci le riparazioni 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 risultato in qualsiasi account e regione in cui è distribuita la soluzione.

Ricevi notifiche sulle azioni correttive e sui risultati

Iscriviti all'SNSargomento Amazon distribuito dalla soluzione per ricevere una notifica quando vengono avviate le riparazioni e se la riparazione ha avuto esito positivo o meno.

Integra con sistemi di ticket come Jira o ServiceNow

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

Utilizzo AWSConfigRemediations nelle partizioni GovCloud e in Cina

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

Estendi la soluzione con correzioni personalizzate e implementazioni di Playbook

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

Casi d'uso

Implementa la conformità a uno standard in tutti gli account e le aree geografiche della tua organizzazione

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

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

Utilizza i componenti Orchestrator forniti come framework. Crea soluzioni personalizzate per gestire le out-of-compliance risorse 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:

applicazione

Un gruppo logico di AWS risorse che si desidera utilizzare come unità.

bonifica, manuale di correzione

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 della funzione Lambda dovrebbero

proibire l'accesso pubblico» modificherebbe la politica della funzione AWS Lambda pertinente per rimuovere le istruzioni che consentono l'accesso pubblico.

control runbook

Uno dei set di documenti di automazione AWS Systems Manager (SSM) utilizzati da Orchestrator per indirizzare una correzione avviata per un controllo specifico al runbook di riparazione corretto. Ad esempio, le riparazioni per SC Lambda.1 e AWS Foundational Security Best Practices (FSBP) Lambda.1 vengono implementate con lo stesso runbook di correzione. L'Orchestrator richiama il runbook di controllo per ogni controllo, che sono denominati rispettivamente - _Lambda.1 e - SC_2.0.0_Lambda.1. ASR AFSBP ASR Ogni runbook di controllo richiama lo stesso runbook di correzione, ASR che RemoveLambdaPublicAccess in questo caso sarebbe -.

orchestratore

Step Functions implementata dalla soluzione che prende come input un oggetto di ricerca da AWS Security Hub e richiama il runbook di controllo corretto nell'account e nella regione di destinazione. L'Orchestrator notifica inoltre alla soluzione SNS Topic quando la riparazione viene avviata e quando la riparazione 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 AWSFSBP.

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 deve vietare l'accesso pubblico. Una funzione che consente 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, quando attivata, mostra i risultati con il relativo controllo consolidato IDs anziché IDs quelli corrispondenti 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 S3.1 sono tutti mappati al controllo consolidato (SC) S3.2 «I bucket S3 dovrebbero vietare l'accesso pubblico in lettura». Quando questa funzionalità è attivata, vengono utilizzati i runbook SC.

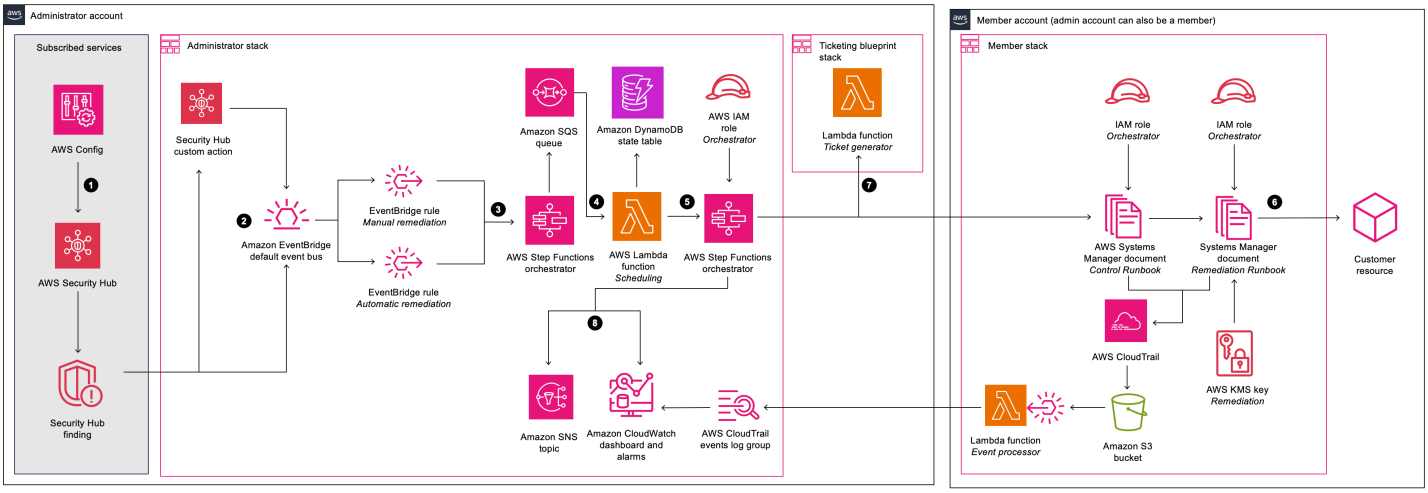
Per un riferimento generale dei AWS termini, consulta il AWS Glossario.

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'AWSarchitettura

> **Note**
>
> AWS CloudFormation le risorse vengono create da costrutti AWS Cloud Development Kit (AWSCDK).

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

1. Detect: AWS Security Huboffre ai clienti una visione completa del loro stato di AWS sicurezza. 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 AWS servizi AWS Config, come Amazon Guard Duty e AWS Firewall Manager. Questi eventi e dati vengono analizzati in base a standard di sicurezza, come CIS AWS Foundations Benchmark. Le eccezioni vengono dichiarate come

risultati nella console. AWS Security Hub Le nuove scoperte vengono inviate come EventBridge eventi Amazon.

2. Avvia: puoi avviare eventi in base ai risultati utilizzando azioni personalizzate, che generano eventi. EventBridge AWS Security Hub le azioni e le EventBridge regole personalizzate avviano la risposta automatica di sicurezza sui AWS playbook per risolvere i risultati. La soluzione implementa:

   a. Una EventBridge regola da abbinare all'evento di azione personalizzato

   b. Una regola di EventBridge evento per ogni controllo supportato (disattivata per impostazione predefinita) in modo che corrisponda all'evento di ricerca in tempo reale

   È possibile utilizzare il menu Azioni personalizzate nella console Security Hub per avviare la riparazione automatica. Dopo attenti test in un ambiente non di produzione, puoi anche attivare le riparazioni automatiche. È possibile attivare le automazioni per le singole riparazioni: non è necessario attivare gli avviamenti automatici per tutte le riparazioni.

3. Pre-riparazione: nell'account amministratore, AWS Step Functionselabora l'evento di riparazione e lo prepara per la pianificazione.

4. Pianificazione: la soluzione richiama la AWS Lambdafunzione di pianificazione per inserire l'evento di riparazione nella tabella di stato di Amazon DynamoDB.

5. Orchestrate: nell'account amministratore, Step Functions utilizza ruoli cross-account AWS Identity and Access Management()IAM. Step Functions richiama la correzione nell'account membro contenente la risorsa che ha prodotto il risultato di sicurezza.

6. Correzione: un documento di AWS Systems Managerautomazione nell'account membro esegue l'azione necessaria per correggere il risultato sulla risorsa di destinazione, ad esempio disabilitando l'accesso pubblico Lambda.

   Facoltativamente, puoi abilitare la funzionalità Action Log negli stack dei membri con il parametro. EnableCloudTrailForASRActionLog Questa funzionalità acquisisce le azioni intraprese dalla soluzione nei tuoi account Membro e le visualizza nella CloudWatch dashboard Amazon della soluzione.

7. (Facoltativo) Crea un ticket: se utilizzi il TicketGenFunctionNameparametro 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 servizio di biglietteria dopo che la riparazione è stata eseguita correttamente nell'account del membro. Forniamo stack per l'integrazione con Jira e. ServiceNow

8. Notifica e registra: il playbook registra i risultati in un gruppo di CloudWatch log, invia una notifica a un argomento di Amazon Simple Notification Service SNS (Amazon) e aggiorna i risultati del Security Hub. La soluzione mantiene una traccia di controllo delle azioni nelle note dei risultati.

AWSConsiderazioni sulla progettazione Well-Architected

Questa soluzione è stata progettata con le migliori pratiche del AWS Well-Architected Framework, che aiuta 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 migliori pratiche del pilastro dell'eccellenza operativa.

- Risorse definite come IaC utilizzando. CloudFormation
- Correzioni implementate con le seguenti caratteristiche, ove possibile:
  - Idempotenza
  - Gestione e segnalazione degli errori
  - Registrazione
  - 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 migliori pratiche del pilastro della sicurezza.

- IAMutilizzato 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 jolly per poter agire su qualsiasi risorsa.

Affidabilità

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'affidabilità.

- Security Hub continua a creare risultati se la causa alla base del risultato non viene risolta mediante 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 migliori pratiche 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 migliori pratiche del pilastro dell'ottimizzazione dei costi.

- I servizi serverless ti consentono di pagare solo ciò che utilizzi.
- Utilizza il livello gratuito per SSM l'automazione 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 la scalabilità verso l'alto o verso il basso in base alle esigenze.

Dettagli dell'architettura

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

AWS Security Hub integrazione

L'implementazione dello `aws-sharr-deploy` stack crea l'integrazione con la funzionalità di azione personalizzata di AWS Security Hub. Quando gli utenti AWS Security Hub della console selezionano Findings for remediation, la soluzione indirizza il record di ricerca per la correzione utilizzando un. AWS Step Functions

Le autorizzazioni e AWS Systems Manager i runbook tra account devono essere distribuiti a tutti gli AWS Security Hub account (amministratore e membro) utilizzando i modelli and. `aws-sharr-member.template` `aws-sharr-member-roles.template` CloudFormation Per ulteriori informazioni, consulta Playbook. Questo modello consente la riparazione automatica nell'account di destinazione.

Gli utenti possono avviare automaticamente riparazioni automatiche in base alla singola riparazione utilizzando le regole degli eventi di Amazon. CloudWatch Questa opzione attiva la correzione completamente automatica dei risultati non appena vengono segnalati. AWS Security Hub Per impostazione predefinita, gli avviamenti automatici sono disattivati. Questa opzione può essere modificata in qualsiasi momento durante o dopo l'installazione del playbook attivando le regole degli CloudWatch eventi nell'account AWS Security Hub amministratore.

Correzione tra account

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

Playbook

Una serie di rimedi 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 la Guida per gli sviluppatori -> Playbooks. Questa soluzione attualmente supporta i seguenti playbook:

- Security Control, un playbook allineato alla funzionalità Consolidated control results di AWS Security Hub, pubblicato il 23 febbraio 2023.

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

- Benchmark di Center for Internet Security (CIS) Amazon Web Services Foundations, versione 1.2.0, pubblicati il 18 maggio 2018.
- Benchmark di Center for Internet Security (CIS) Amazon Web Services Foundations, versione 1.4.0, pubblicati il 9 novembre 2022.
- Benchmark di 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 a novembre 2023.

Registrazione centralizzata

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

Notifiche

Questa soluzione utilizza un argomento Amazon Simple Notification Service (AmazonSNS) per pubblicare i risultati delle riparazioni. 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.

AWSservizi inclusi in questa soluzione

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

AWS servizio	Descrizione
Amazon EventBridge	Nucleo. Implementa eventi che avvieranno la funzione orchestator step quando viene corretto un risultato.
AWS IAM	Nucleo. Implementa molti ruoli per consentire riparazioni su risorse diverse.
AWS Lambda	Core. Implementa più funzioni lambda che verranno utilizzate dallo step function orchestat or per risolvere i problemi.
AWS Security Hub	Core. Fornisce ai clienti una visione completa del loro stato AWS di sicurezza.
AWS Step Functions	Nucleo. Implementa un orchestratore che richiamerà i documenti di riparazione con chiamate Systems Manager. AWS API
AWS Systems Manager	Nucleo. Implementa i documenti di System Manager (collegamento al documento) che contengono la logica di riparazione che verrà eseguita.
AWS CloudTrail	Supporto. Registra le modifiche apportate dalla soluzione alle AWS risorse e le visualizza su una CloudWatch dashboard.
Amazon CloudWatch	Supporto. Implementa gruppi di log che i diversi playbook utilizzeranno per registrare i risultati

AWS servizio	Descrizione
	. Raccoglie metriche da visualizzare su una dashboard personalizzata con allarmi.
AWS DynamoDB	Supporto. Memorizza l'ultima correzione eseguita in ogni account e regione per ottimizza re la pianificazione delle riparazioni.
Service Catalog AppRegistry	Supporto. Implementa un'applicazione per gli stack distribuiti per tenere traccia dei costi e dell'utilizzo.
Amazon Simple Notification Service	Supporto. Implementa SNS argomenti che ricevono una notifica una volta completata una correzione.
AWS SQS	Supporto. Aiuta a pianificare le riparazioni in modo che la soluzione possa eseguire le riparazioni in parallelo.

Pianifica la tua implementazione

Questa sezione descrive i costi, la sicurezza della rete, il supporto Regioni AWS, le quote e altre considerazioni prima dell'implementazione della soluzione.

Costo

Sei responsabile del costo dei AWS servizi utilizzati per eseguire questa soluzione. A partire da questa revisione, il costo per l'esecuzione di questa soluzione con le impostazioni predefinite negli Stati Uniti orientali (Virginia settentrionale) Regione AWS è di circa 21,17 USD per 300 riparazioni al mese, 134,86 USD per 3.000 riparazioni/mese e 1.281,01 USD per 30.000 riparazioni/mese. I prezzi sono soggetti a modifiche. Per tutti i dettagli, consulta la pagina dei prezzi di ogni servizio utilizzato in questa soluzione AWS .

> **Note**
>
> Molti AWS servizi 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 prezzo forniti.

Ti consigliamo di creare un budgetAWS Cost Explorer per facilitare la gestione dei costi. I prezzi sono soggetti a modifiche. Per tutti i dettagli, consulta la pagina web dei prezzi di ogni AWS servizio utilizzato in questa soluzione.

Esempio di tabella dei costi

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

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

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

Servizio	Livello gratuito	Prezzi [USD]
AWS Systems Manager Automation - Step Count	100.000 passaggi per account al mese	Oltre al piano gratuito, ogni passaggio base viene addebitato a 0,002 USD per passaggio. Per le automazioni con più account, tutti i passaggi, inclusi quelli eseguiti in qualsiasi account per bambini, vengono conteggiati solo nell'account di origine.
AWS Systems Manager Automation - Durata della fase	5.000 secondi al mese	Oltre al piano gratuito, ogni fase di aws: executeScript action viene addebitata a 0,00003 USD al secondo dopo un piano gratuito di 5.000 secondi al mese.
AWS Systems Manager Automation - Archiviazione	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) out-of-Region
AWS Security Hub - Controlli di sicurezza	Nessun livello gratuito	I primi 100.000 dollari checks/account/Region/month costano 0,0010 USD per assegno I successivi 400.000 dollari checks/account/Region/month costano 0,0008 USD per assegno Oltre 500.000 dollari checks/account/Region/month

Servizio	Livello gratuito	Prezzi [USD]
		costano 0,0005 USD per assegno
AWS Security Hub - Ricerca degli eventi di ingestione	I primi 10.000€ sono events/account/Region/month gratuiti. Individuazione degli eventi di ingestione associati ai controlli di sicurezza di Security Hub.	Oltre 10.000 dollari events/account/Region/month costano 0,00003 dollari per evento
Amazon CloudWatch - Metriche	Metriche di monitoraggio di base (con frequenza di 5 minuti) 10 parametri di monitoraggio dettagliati (con frequenza di 1 minuto) 1 milione di API richieste (non applicabile a e) GetMetricData GetMetricWidgetImage	I primi 10.000 parametri costano 0,30 dollari metrici al mese Le successive 240.000 metriche costano 0,10 USD metrici al mese I successivi 750.000 parametri costano 0,05 USD metrici al mese Oltre 1.000.000 di parametri costano 0,02 USD metrici al mese APIle chiamate costano 0,01 USD per 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	Livello gratuito	Prezzi [USD]
Amazon CloudWatch - Allarmi	10 parametri di allarme (non applicabile agli allarmi ad alta risoluzione)	La risoluzione standard (60 sec) costa 0,10 USD per 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 materiale composito costa 0,50 USD per allarme
Amazon CloudWatch - Raccolta di registri	5 GB di dati (acquisizione, archiviazione e scansione dei dati mediante query di Logs Insights)	0,50 USD per GB
Amazon CloudWatch - Archiviazione dei log	5 GB di dati (acquisizione, archiviazione e scansione dei dati mediante query di Logs Insights)	0,005 USD per GB di dati scansionati
Amazon CloudWatch - Eventi	Sono inclusi tutti gli eventi tranne gli eventi personalizzati	1,00 USD per milione di eventi per eventi personalizzati 1,00 USD per milione di eventi per eventi tra più account
AWS Lambda - Richieste	1 milione di richieste gratuite al mese	0,20 USD per 1 milione di richieste

Servizio	Livello gratuito	Prezzi [USD]
AWS Lambda - Durata	400.000 GB di tempo di elaborazione al mese	0,0000166667 USD per ogni GB al secondo. Il prezzo di Duration dipende dalla quantità di memoria allocata alla funzione. È possibile allocare qualsiasi quantità di memoria alla funzione tra 128 MB e 10.240 MB, con incrementi di 1 MB.
AWS Step Functions - Transizioni di stato	4.000 transizioni statali gratuite al mese	0,025 USD per 1.000 transizioni di stato successive
Amazon EventBridge	Tutti gli eventi di cambiamento di stato pubblicati dai servizi sono gratuiti AWS	Gli eventi personalizzati costano 1,00 USD per milione di eventi personalizzati pubblicati Gli eventi di terze parti (SaaS) costano 1,00 USD per milione di eventi pubblicati Gli eventi su più account costano 1,00 USD per milione di eventi inviati su più account
Amazon SNS	I primi 1 milione di SNS richieste Amazon al mese sono gratuite	0,50 USD per 1 milione di richieste successive
Amazon SQS	I primi 1 milione di SQS richieste Amazon al mese sono gratuite	0,40 USD per ogni milione o 100 miliardi di richieste successive

Servizio	Livello gratuito	Prezzi [USD]
Amazon DynamoDB	I primi 25 GB di spazio di archiviazione sono gratuiti	2,00 USD per 1 milione di letture e scritture coerenti successive

Esempi di prezzi (mensili)

Esempio 1:300 riparazioni al mese

- 10 account, 1 regione
- 30 riparazioni per account/Region/month
- Costo totale 21,17 USD al mese

Servizio	Ipotesi	Spese mensili [] USD
AWS Systems Manager Automation	Passaggi: ~4 passaggi* 300 riparazioni* 0,002 USD = 2,40 USD Durata: 10 sec* 300 riparazioni * 0,00003 USD = 0,09 USD	2,49 USD
AWS Security Hub	Nessun servizio fatturabile utilizzato	0 USD
CloudWatch Registri Amazon	300 riparazioni* 0,000002 USD = 0,0006 USD 0,0006 USD* 0,03 = 0,000018 USD	< 0,01 US$
AWS Lambda - Richieste	300 riparazioni* 6 richieste = 1.800 richieste	0,20 US$

Servizio	Ipotesi	Spese mensili [] USD
	0,20 USD* 1.000.000 di richieste = 0,20 USD	
AWS Lambda - Durata	256 MB: 1,875 GB sec* 300 riparazioni* 0,0000167 USD = 0,009375 USD	< 0,01 USD
AWS Step Functions	17 transizioni di stato * 300 riparazioni = 5.100 0,025 USD* (5.100/1.000) transizioni di stato = 0,15 USD	$0,15
EventBridge Regole di Amazon	Nessun costo per le regole	0 USD
AWS Key Management Service	1 chiave* 10 account* 1 regione* 1$ = 10$	$10,00
Amazon DynamoDB	2,00 USD* 1.000.000 di letture e scritture = 2,00 USD	$2,00
Amazon SQS	0,40 USD* 1.000.000 di richieste = 0,40 USD	0,40 US$
Amazon SNS	0,50 USD* 1.000.000 di notifiche = 0,50 USD	$0,50
Amazon CloudWatch - Metriche	0,30 USD* 7 metriche personalizzate = 2,10 USD 0,01 USD* (300 * 3/1.000) chiamate put metriche = 0,01 USD API	2,11 USD
Amazon CloudWatch - Pannelli di controllo	3,00 USD* 1 dashboard = 3,00 USD	$3,00

Servizio	Ipotesi	Spese mensili [] USD
Amazon CloudWatch — Allarmi	0,10 USD* 3 allarmi = 0,30 USD	0,30$
Totale		21,17$

Esempio 2:3.000 riparazioni al mese

- 100 account, 1 regione
- 30 riparazioni per account/Region/month
- Costo totale 134,86 USD al mese

Servizio	Ipotesi	Spese mensili [] USD
AWS Systems Manager Automation	Passaggi: ~4 passaggi * 3.000 riparazioni* 0,002 USD = 24,00 USD Durata: 10 sec* 3.000 riparazioni* 0,00003 USD = 0,90 USD	$24,90
AWS Security Hub	Nessun servizio fatturabile utilizzato	0 USD
CloudWatch Registri Amazon	3.000 riparazioni* 0,000002 USD = 0,006 USD 0,006 USD* 0,03 = 0,00018 USD	< 0,01 US$
AWS Lambda - Richieste	3.000 riparazioni* 6 richieste = 18.000 richieste 0,20 USD* 1.000.000 di richieste = 0,20 USD	0,20 US$

Servizio	Ipotesi	Spese mensili [] USD
AWS Lambda - Durata	256 milioni: 1,875 GB sec* 3.000 riparazioni* 0,000167 USD = 0,09375 USD	0,09 USD
AWS Step Functions	17 transizioni di stato * 3.000 riparazioni = 51.000 0,025 USD* (51.000/1.000) transizioni di stato = 1,275 USD	$1,28
EventBridge Regole di Amazon	Nessun costo per le regole	0 USD
AWS Key Management Service	1 chiave* 100 account* 1 regione* 1$ = 100$	$100
Amazon DynamoDB	2,00 USD* 1.000.000 di letture e scritture = 2,00 USD	$2,00
Amazon SQS	0,40 USD* 1.000.000 di richieste = 0,40 USD	0,40 US$
Amazon SNS	0,50 USD* 1.000.000 di notifiche = 0,50 USD	$0,50
Amazon CloudWatch - Metriche	0,30 USD* 7 metriche personalizzate = 2,10 USD 0,01 USD* (3000 * 3/1.000) chiamate put metriche = 0,09 USD API	2,19 USD
Amazon CloudWatch - Pannelli di controllo	3,00 USD* 1 dashboard = 3,00 USD	$3,00

Servizio	Ipotesi	Spese mensili [] USD
Amazon CloudWatch — Allarmi	0,10 USD* 3 allarmi = 0,30 USD	0,30$
Totale		$134,86

Esempio 3:30.000 riparazioni al mese

- 1.000 account, 1 regione
- 30 riparazioni per account/Region/month
- Costo totale 1.281,01 USD al mese

Servizio	Ipotesi	Spese mensili [] USD
AWS Systems Manager Automation	Fasi: ~4 passaggi* 30.000 riparazioni* 0,002 USD = 240,00 USD Durata: 10 sec* 30.000 riparazioni* 0,00003 USD = 9,00 USD	249,00$
AWS Security Hub	Nessun servizio fatturabile utilizzato	0 USD
CloudWatch Registri Amazon	30.000 riparazioni* 0,000002 USD = 0,06 USD 0,06 USD* 0,03 = 0,0018 USD	< 0,01 US$
AWS Lambda - Richieste	30.000 riparazioni* 6 richieste = 180.000 richieste 0,20 USD* 1.000.000 di richieste = 0,20 USD	0,20 US$

Servizio	Ipotesi	Spese mensili [] USD
AWS Lambda - Durata	256 milioni: 1,875 GB sec* 30.000 riparazioni* 0,000167 USD = 0,9375 USD	0,94 USD
AWS Step Functions	17 transizioni di stato* 30.000 riparazioni = 510.000 0,025 USD* (510.000/1.000) transizioni di stato = 12,75 USD	$12,75
EventBridge Regole di Amazon	Nessun costo per le regole	0 USD
AWS Key Management Service	1 chiave* 1.000 account* 1 regione* 1$ = 1.000 USD	1.000$
Amazon DynamoDB	0,000002 USD * 1.000.000 di operazioni di lettura e scrittura = 2,00 USD	$2,00
Amazon SQS	0,000004 USD* 1.000.000 di richieste = 0,40 USD	0,40 US$
Amazon SNS	0,000005 USD * 1.000.000 di notifiche = 0,50 USD	0,50 USD
Amazon CloudWatch - Metriche	0,30 USD* 6 metriche personalizzate = 1,80 USD 0,01 USD* (30.000 * 3/1.000) chiamate put metrics = 0,90 USD API	2,70$
Amazon CloudWatch - Pannelli di controllo	3,00 USD* 1 dashboard = 3,00 USD	$3,00

Servizio	Ipotesi	Spese mensili [] USD
Amazon CloudWatch — Allarmi	0,10 USD* 2 allarmi = 0,20 USD	0,20$
Amazon CloudWatch — Approfondimenti sulle applicazioni	0,10 USD* 40 allarmi (max) = 4,00 USD 0,53 USD* 10 GB di dati di registro (stimati) = 5,30 USD 0,00267 US$ * 5 OpsItems (stimati) = ~$0,01	$9,31
Totale		$1.281,01

Costo aggiuntivo per le funzionalità opzionali

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

Metriche avanzate CloudWatch

Se si seleziona `yes` il EnableEnhancedCloudWatchMetricsparametro durante la distribuzione dello stack di amministrazione, la soluzione crea due metriche personalizzate e un allarme per ogni ID di controllo. Il costo dipende dal numero di controlli da IDs correggere. Nella tabella seguente, si presume che si stiano ripristinando tutti i 96 diversi controlli IDs al mese, per determinare il limite massimo dei costi.

Servizio	Ipotesi 96 controlli IDs * 2 = 192 metriche personalizzate	Spese mensili [] USD
Amazon CloudWatch - Metriche	0,30 USD* 192 metriche personalizzate = 57,60 USD	57,60$
Amazon CloudWatch - Allarmi	0,10 USD* 96 allarmi = 9,60 USD	9,60$

Servizio	Ipotesi	Spese mensili [] USD
	96 controlli IDs * 2 = 192 metriche personalizzate	
Totale		$67,20

CloudTrail Registro delle azioni

In ogni account membro per cui abiliti la funzionalità Action Log, le soluzioni creano una CloudTrail traccia 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 nell'account, poiché gli eventi non correlati alla soluzione vengono comunque acquisiti dal trail 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 nell'account.

Servizio	Ipotesi	Spese mensili [] USD
AWS CloudTrail	150.000 USD* 2,00/100.000 USD = 3,00 USD	$3,00
Lambda	150.000 * 0,2 * 0,125 = 3.750 GB/secondi 3.750 USD* 0,0000166667 = 0,0625 USD di costo del tempo di elaborazione 0,15 USD* 0,20 USD = 0,03 USD per il costo della richiesta 0,0625 USD + 0,03 USD = 0,0952 USD di costo totale Lambda	0,0925 USD
Totale		3,09$ per account membro

Sicurezza

Quando crei sistemi sull'AWSinfrastruttura, le responsabilità in materia di sicurezza vengono condivise tra te eAWS. Questo modello condiviso riduce il carico operativo perché AWS 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 AWS sicurezza, visita il sito AWSCloud Security.

Ruoli IAM

AWSI ruoli 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 IAM ruoli che garantiscono alle funzioni automatizzate della soluzione l'accesso per eseguire azioni di riparazione entro un ambito ristretto di autorizzazioni specifiche per ciascuna riparazione.

La Step Function dell'account amministratore è assegnata al ruolo SO0111-. SHARR-Orchestrator-Admin Solo questo ruolo può assumere il membro SO0111-Orchestrator in ogni account membro. Il ruolo membro è autorizzato da ciascun ruolo di riparazione a 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-R emoveVPCDefault SecurityGroupRules è il ruolo del runbook di correzione -R. ASR emoveVPCDefault SecurityGroupRules

Supportato Regioni AWS

Nome 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
US West (Oregon)	us-west-2
Africa (Cape Town)	af-south-1
Asia Pacifico (Hong Kong)	ap-east-1

Nome Regione	Codice regione
Asia Pacific (Hyderabad)	ap-south-2
Asia Pacifico (Giacarta)	ap-southeast-3
Asia Pacifico (Melbourne)	ap-southeast-4
Asia Pacific (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
Europa (Milano)	eu-south-1
Europe (Paris)	eu-west-3
Europa (Spagna)	eu-south-2
Europa (Stoccolma)	eu-north-1
Europa (Zurigo)	eu-central-2
Medio Oriente (Bahrein)	me-south-1
Medio Oriente () UAE	me-central-1

Nome Regione	Codice regione
Sud America (San Paolo)	sa-east-1
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1
AWS GovCloud (Stati Uniti occidentali)	us-gov-east-2
China (Beijing)	cn-north-1
China (Ningxia)	cn-northwest-1

Quote

Le quote di servizio, a cui si fa riferimento anche come limiti, rappresentano il numero massimo di risorse di servizio o operazioni per l'account AWS.

Quote per i AWS servizi di questa soluzione

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

Utilizza i seguenti collegamenti per accedere alla pagina relativa al servizio. Per visualizzare le Service Quotas per tutti i AWS servizi nella documentazione senza cambiare pagina, visualizza invece le informazioni nella pagina Service Endpoints and quotas. PDF

AWS CloudFormation quote

Il tuo AWS account ha delle AWS CloudFormation quote di cui dovresti essere a conoscenza quando avvii lo stack di questa soluzione. Comprendendo queste quote, è possibile evitare errori di limitazione che impedirebbero di implementare correttamente questa soluzione. Per ulteriori informazioni, consultare Quote di AWS CloudFormation nella Guida per l'utente di AWS CloudFormation .

Amazon EventBridge regola le quote

Il tuo AWS account prevede EventBridge delle quote di regole Amazon di cui devi essere a conoscenza quando selezioni i playbook da distribuire con la soluzione. Ogni playbook creerà una EventBridge regola per ogni controllo a cui può porre rimedio. Quando si distribuiscono più playbook,

è possibile raggiungere la quota di regole. Per ulteriori informazioni, consulta le EventBridge quote Amazon nella Amazon EventBridge User Guide.

AWSImplementazione del Security Hub

AWSL'implementazione e la configurazione di Security Hub sono un prerequisito per questa soluzione. Per ulteriori informazioni sulla configurazione di AWS Security Hub, consulta Configurazione del AWS Security Hub nella Guida per l'utente AWS di Security Hub.

Come minimo, devi avere un Security Hub funzionante configurato nel tuo account principale. È possibile distribuire questa soluzione nello stesso account (e AWS regione) dell'account primario di Security Hub. In ogni account primario e secondario di Security Hub, è inoltre necessario distribuire il modello di membro che consente AssumeRole le autorizzazioni a AWS Step Functions della soluzione per eseguire i runbook di correzione nell'account.

Stack vs implementazione StackSets

Un set di stack consente di creare stack in AWS account di diverse AWS regioni utilizzando un unico modello. AWS CloudFormation A partire dalla versione 1.4, questa soluzione supporta l'implementazione di stack set suddividendo le risorse in base a dove e come vengono distribuite. I clienti con più account, in particolare quelli che utilizzano AWS Organizations, possono trarre vantaggio dall'utilizzo di set di stack per la distribuzione su più account. Riduce lo sforzo necessario per l'installazione e la manutenzione della soluzione. Per ulteriori informazioni su StackSets, fare riferimento a Uso AWS CloudFormation StackSets.

Implementa la soluzione

> **Important**
>
> Se la funzionalità dei risultati del controllo consolidato è attivata in Security Hub (impostazione predefinita nelle nuove distribuzioni), abilita il playbook Security Control (CS) solo quando distribuisci questa soluzione. Se la funzione non è attivata, abilita solo i playbook per gli standard di sicurezza abilitati in Security Hub. L'attivazione di playbook aggiuntivi può comportare il raggiungimento della quota per EventBridge le regole.

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

Affinché la soluzione funzioni, è necessario implementare 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 distribuire ogni stack come stack o. StackSet

Decidere dove distribuire ogni stack

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

- Admin stack: funzione Orchestrator Step, regole degli eventi e azione personalizzata del Security Hub.
- Member stack: documenti di Remediation Automation. SSM
- Stack di ruoli dei membri: IAM ruoli per le riparazioni.

Lo stack di amministrazione deve essere distribuito una sola volta, in un unico account e in un'unica regione. Deve essere distribuito nell'account e nella regione che hai configurato come destinazione di aggregazione per i risultati del Security Hub per la tua organizzazione.

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

Ad esempio, un'organizzazione ha account che operano nelle regioni `us-east-1` e`us-west-2`, con 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 `111111111111` amministratore delegato. Tutti e tre gli account devono essere configurati per aggregare i risultati dal `us-west-2` al. `us-east-1` Lo stack di amministrazione deve essere distribuito sull'account in. `111111111111` `us-east-1`

Per maggiori dettagli sulla ricerca dell'aggregazione, consulta la documentazione per gli account 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 tra gli account dei membri e l'account hub.

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

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 (`111111111111222222222222`, e) e su entrambe le regioni (e`333333333333`). `us-east-1` `us-west-2`

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

Utilizzando l'esempio precedente, suggeriamo di distribuire lo stack di ruoli dei membri su tutti e tre gli account (, e) in. `111111111111` `222222222222` `333333333333` `us-east-1`

Decidere come distribuire ogni stack

Le opzioni per distribuire uno stack sono

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

StackSets con autorizzazioni gestite dal servizio sono le più comode perché non richiedono l'implementazione di ruoli propri e possono essere implementate automaticamente su nuovi account dell'organizzazione. Sfortunatamente, questo metodo non supporta gli stack annidati, che utilizziamo 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 durante la distribuzione all'intera organizzazione, l'account di gestione dell'organizzazione non è incluso, quindi se desideri correggere i risultati nell'account di gestione dell'organizzazione, devi distribuirlo su questo account separatamente.

Lo stack di membri deve essere distribuito su ogni account e regione, ma non può essere distribuito utilizzando autorizzazioni gestite dal servizio perché contiene stack StackSets annidati. Pertanto, suggeriamo di distribuire questo stack con autorizzazioni gestite automaticamente. StackSets

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

Risultati di controllo consolidati

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

> **Important**
>
> Se abilitata, è necessario utilizzare la versione 2.0.0 della soluzione o successiva. Inoltre, è necessario distribuire gli stack annidati Admin e Member per gli standard «SC» o «security control». In questo modo vengono implementati i documenti e EventBridge le regole di automazione da utilizzare con il controllo consolidato IDs generato quando questa funzionalità è attivata. Non è necessario implementare gli stack annidati Admin o Member per standard specifici (ad esempio) quando si utilizza questa funzionalità. AWS FSBP

AWS CloudFormation modelli

View template

aws-sharr-deploy.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 AWS Step Functions i log e uno stack nidificato 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 Systems AWS Manager.

Supporto per account amministrativi

I seguenti modelli vengono installati nell'account amministratore AWS di Security Hub per attivare gli standard di sicurezza che si desidera supportare. È possibile scegliere quale dei seguenti modelli installare durante l'installazione di`aws-sharr-deploy.template`.

aws-sharr-orchestrator-log.template: crea un gruppo di CloudWatch log per la funzione Orchestrator Step.

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

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

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

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

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

SCStack.template - regole SC v2.0.0.

Account membri

View template

aws-sharr-member.template: utilizza questo modello dopo aver configurato la soluzione principale per installare i runbook di automazione e le autorizzazioni di AWS Systems Manager in ciascuno degli account membro del AWS Security Hub (incluso l'account amministratore). Questo modello consente di scegliere quali playbook standard di sicurezza installare.

`aws-sharr-member.template`Installa i seguenti modelli in base alle tue selezioni:

aws-sharr-remediations.template: codice di correzione comune utilizzato da uno o più standard di sicurezza.

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

CIS120 MemberStack .template - Benchmark di CIS Amazon Web Services Foundations, impostazioni, autorizzazioni e runbook di correzione della versione 1.2.0.

CIS140 MemberStack .template - Benchmark di CIS Amazon Web Services Foundations, impostazioni, autorizzazioni e runbook di correzione della versione 1.4.0.

PCI321MemberStack.template - PCI - Impostazioni, autorizzazioni e runbook di correzione della DSS versione 3.2.1.

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

SCMemberStack.template: impostazioni, autorizzazioni e runbook di correzione del controllo di sicurezza.

Ruoli dei membri

aws-sharr-member-roles.template: definisce i ruoli di riparazione necessari in ogni AWS Security Hub account membro.

Integrazione del sistema di ticket

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

JiraBlu

esegui l'implementazione se usi Jira come sistema di ticketing.

Service

implementalo se lo utilizzi come sistema di ticketing. ServiceNow

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

Implementazione automatizzata - StackSets

> **Note**
>
> Si consiglia di eseguire la distribuzione con. StackSets Tuttavia, per le implementazioni con account singolo o per scopi di test o valutazione, prendi in considerazione l'opzione di distribuzione in stack.

Prima di avviare la soluzione, esaminate l'architettura, i componenti della soluzione, la sicurezza e le considerazioni sulla progettazione discusse in questa guida. Segui le step-by-step istruzioni in questa sezione per configurare e distribuire la soluzione nel tuo. AWS Organizations

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

Prerequisiti

AWSOrganizations ti aiuta a gestire e governare centralmente AWS l'ambiente e le risorse multi-account. StackSets funzionano meglio con AWS Organizations.

Se hai già distribuito la versione 1.3.x o una versione precedente di questa soluzione, devi disinstallare la soluzione esistente. Per ulteriori informazioni, consulta Aggiornare la soluzione.

Prima di implementare questa soluzione, esamina la distribuzione del AWS Security Hub:

- Nell'AWSorganizzazione 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 la sezione Aggregazione dei risultati tra le regioni nella Guida per l'utente del AWS Security Hub.
- È necessario attivare Security Hub per la propria organizzazione in ogni regione in cui si AWS utilizza.

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

Panoramica della distribuzione

> **Note**
>
> StackSets l'implementazione di questa soluzione utilizza una combinazione di gestione dei servizi e gestione automatica. StackSets La modalità Self-Managed StackSets deve essere utilizzata attualmente in quanto utilizza sistemi annidati StackSets, che non sono ancora supportati con Service-Managed. StackSets

Distribuiscili StackSets da un account amministratore delegato nel tuo. AWS Organizations

Pianificazione

Utilizza il seguente modulo per aiutarti con StackSets la distribuzione. 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) Fase 0: Implementazione dello 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: avviare lo stack di amministrazione nell'account amministratore delegato di Security Hub

- Utilizzando un programma autogestito StackSet, avvia il `aws-sharr-deploy.template` AWS CloudFormation modello nel tuo account amministratore AWS di Security Hub nella stessa regione dell'amministratore del Security Hub. Questo modello utilizza pile annidate.
- Scegli quali standard di sicurezza installare. Per impostazione predefinita, è selezionato solo SC (consigliato).
- Scegliete un gruppo di log di Orchestrator esistente da utilizzare. Seleziona `Yes` se esiste `SO0111-SHARR- Orchestrator` già da un'installazione precedente.

Per ulteriori informazioni sulla gestione automatica StackSets, consulta Concedere autorizzazioni autogestite nella Guida per l'AWS CloudFormation utente.

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

Attendi il passaggio 1 per completare la distribuzione, poiché il modello nel passaggio 2 fa riferimento ai IAM ruoli creati dal passaggio 1.

- Utilizzando un servizio gestito StackSet, avvia il `aws-sharr-member-roles.template` AWS CloudFormation modello in un'unica regione in ogni account del tuo. AWS Organizations
- Scegli di installare questo modello automaticamente quando un nuovo account si unisce all'organizzazione.
- Inserisci l'ID dell'account del tuo account AWS Security Hub amministratore.

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

- Utilizzando la gestione automatica StackSets, avvia il `aws-sharr-member.template` AWS CloudFormation modello in tutte le regioni in cui AWS le risorse di ogni account AWS dell'organizzazione sono gestite dallo stesso amministratore del Security Hub.

> **Note**
>
> Fino a quando il StackSets supporto gestito dal servizio non sarà annidato, è necessario eseguire questo passaggio per tutti i nuovi account che entrano a far parte dell'organizzazione.

- Scegliete quali playbook Security Standard installare.
- Fornisci il nome di un gruppo di CloudTrail log (utilizzato per alcune soluzioni correttive).
- Inserisci l'ID dell'account AWS Security Hub amministratore.

(Facoltativo) Fase 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 oppure ServiceNow usali come modello per implementare la tua integrazione personalizzata.

   Per distribuire lo stack Jira:

   a. Inserisci un nome per lo stack.

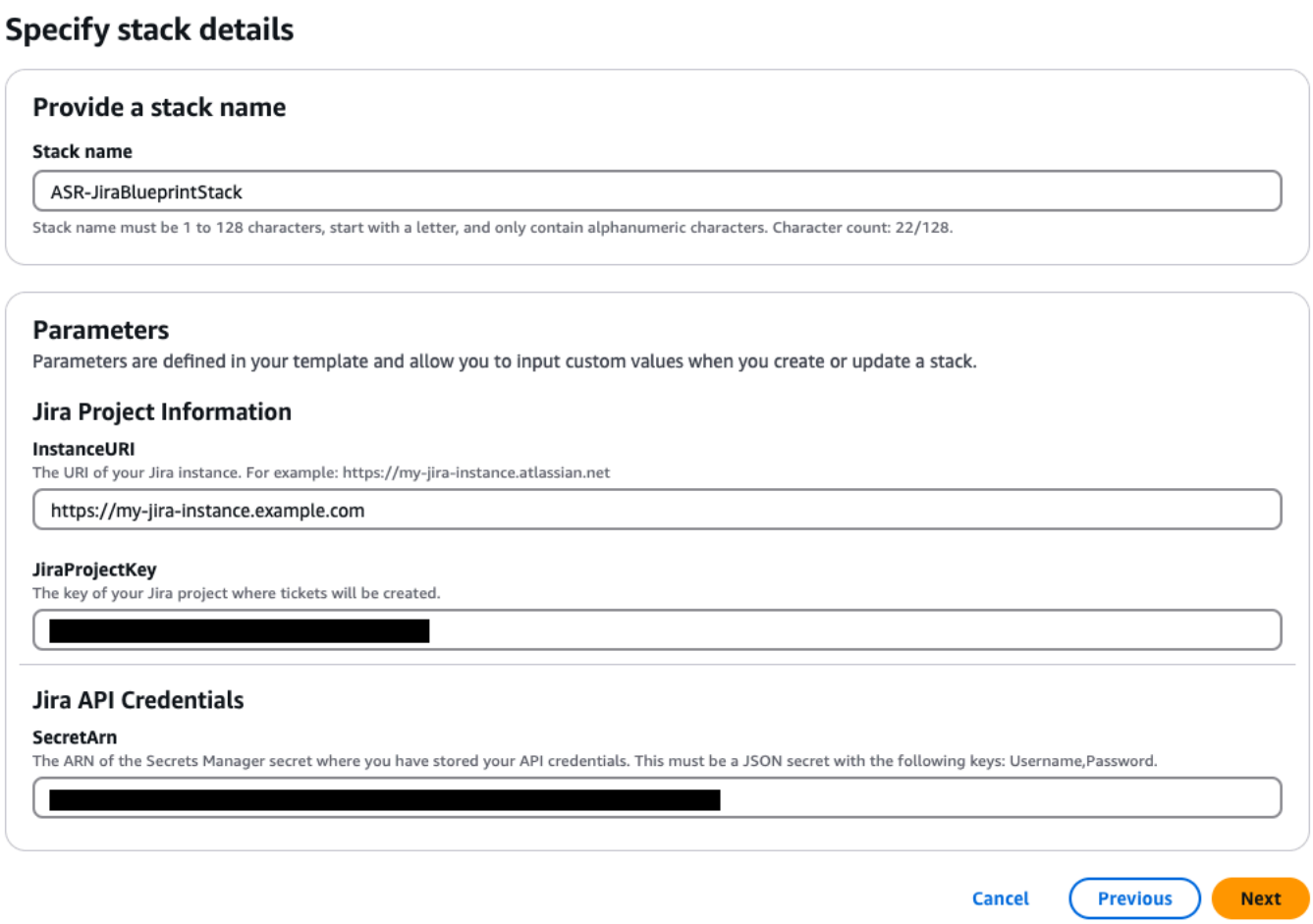
   b. Forniscilo URI alla tua istanza Jira.

   c. Fornisci la chiave del progetto Jira a cui desideri inviare i ticket.

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

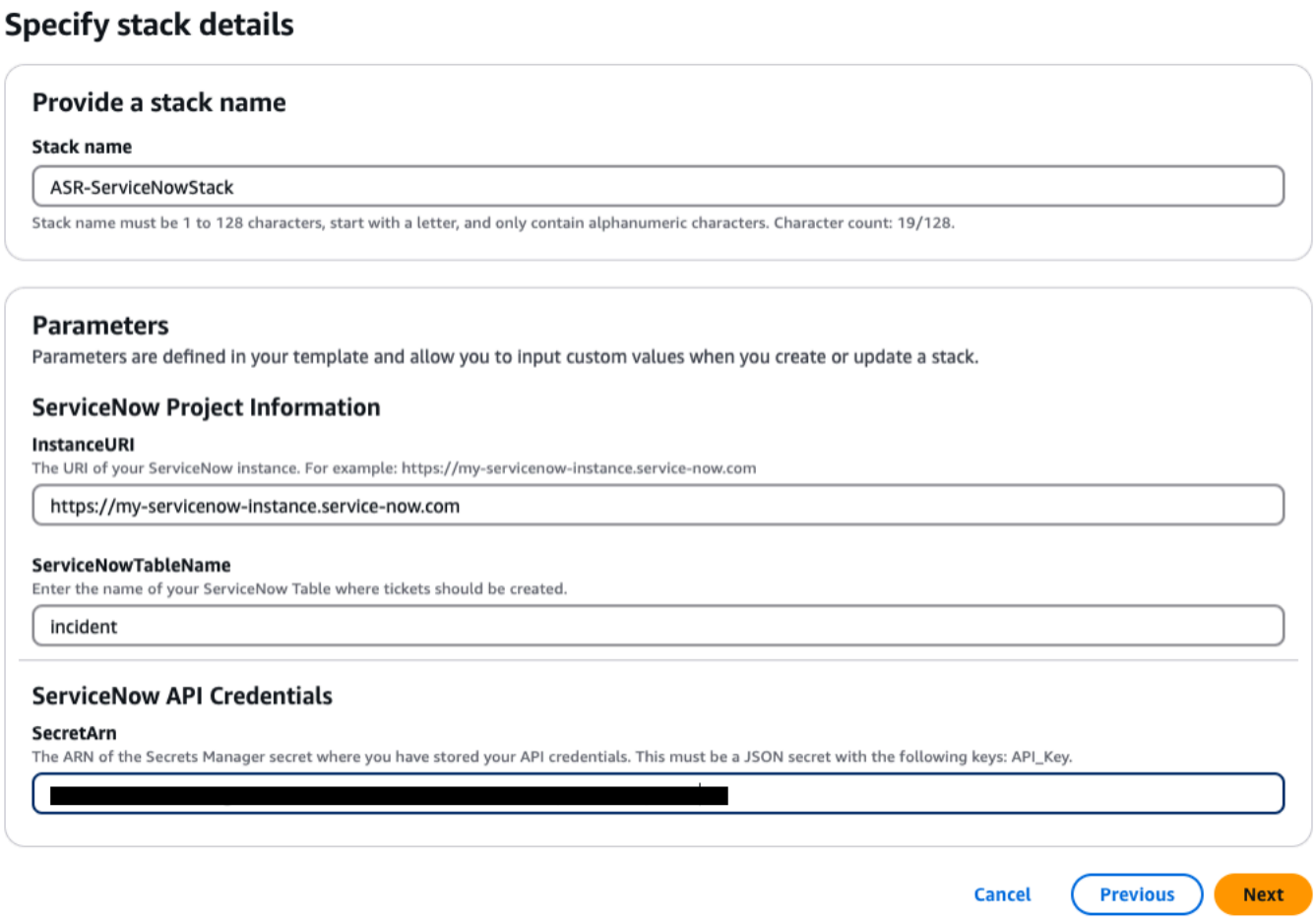
   > **Note**
   >
   > Puoi scegliere di utilizzare una API chiave Jira al posto della password fornendo il tuo nome utente come `Username` e la chiave come. API `Password`

   e. Aggiungi questo segreto come input allo stack. ARN



Per distribuire lo stack: ServiceNow

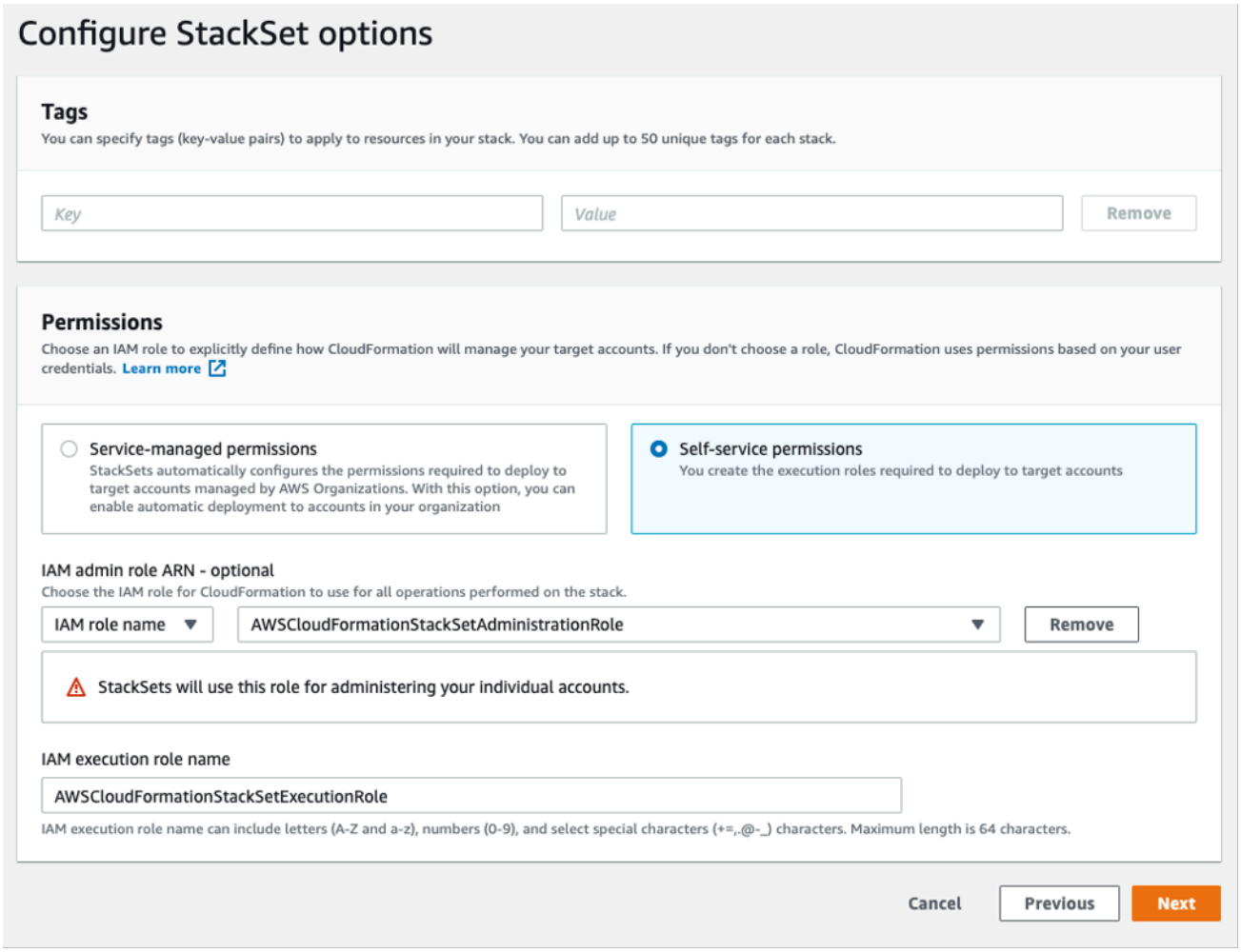
a. Inserisci un nome per lo stack.
b. Fornisci il nome URI della tua ServiceNow istanza.
c. Fornisci il nome della ServiceNow tabella.
d. Crea una API chiave ServiceNow con il permesso di modificare la tabella su cui intendi scrivere.
e. Crea un segreto in Secrets Manager con la chiave `API_Key` e fornisci il segreto ARN come input per lo stack.



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

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

1. Avvia lo stack di amministrazione con `aws-sharr-deploy.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 come sistema autogestito. StackSet



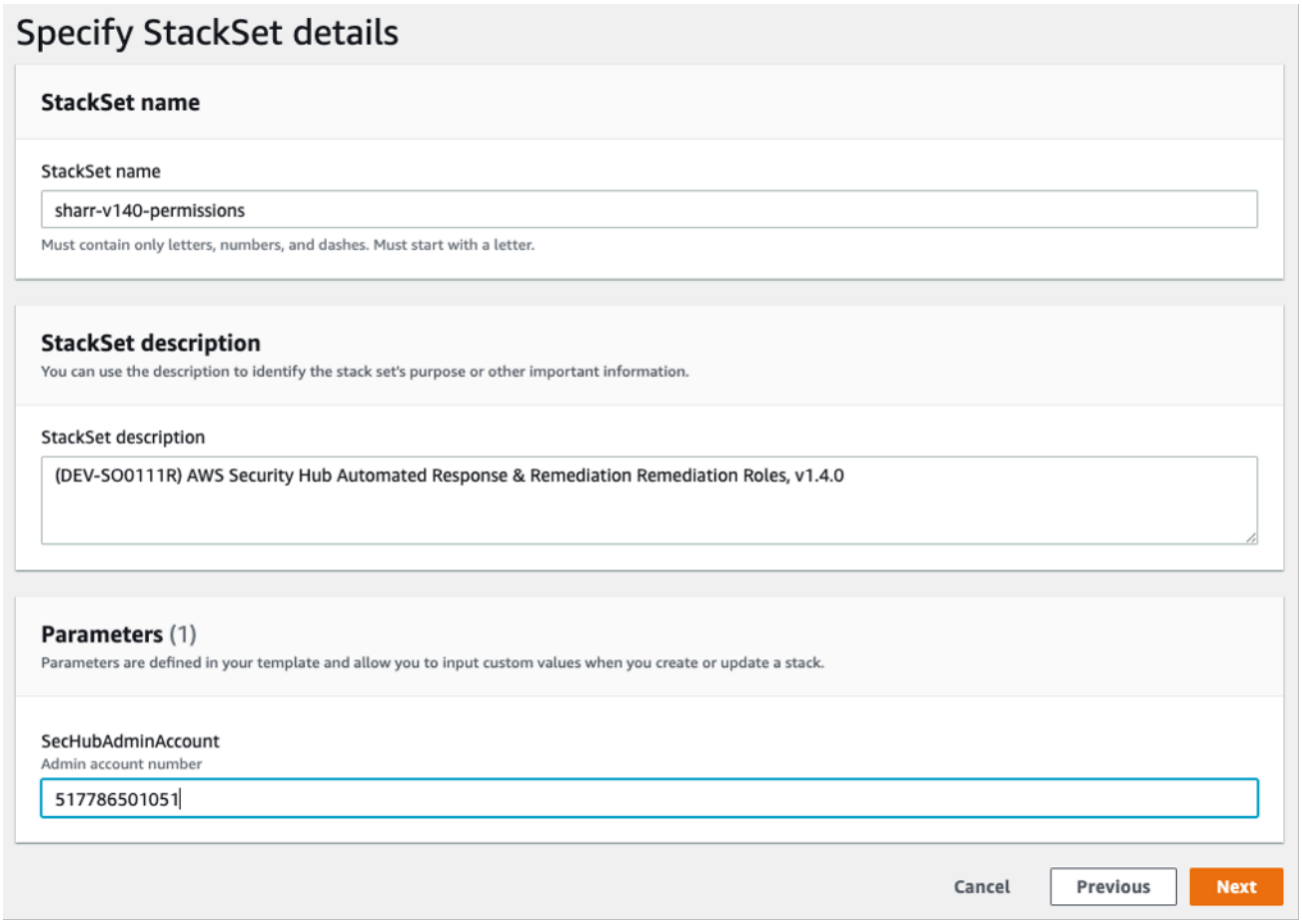
Configurare StackSet le opzioni

2. Per il parametro Account numbers, inserisci l'ID account dell'account amministratore di AWS Security Hub.
3. Per il parametro Specificare le regioni, selezionare solo la regione in cui è attivato l'amministratore di Security Hub. Attendi il completamento di questo passaggio prima di passare al Passaggio 2.

Fase 2: Installare i ruoli di riparazione in ogni account membro del AWS Security Hub

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

1. Effettua la distribuzione all'intera organizzazione (tipica) o alle unità organizzative, in base alle politiche dell'organizzazione.
2. Attiva la distribuzione automatica in modo che i nuovi account nelle AWS Organizzazioni ricevano queste autorizzazioni.
3. Per il parametro Specificare le regioni, seleziona una singola regione. IAMi ruoli sono globali. È possibile continuare con la Fase 3 durante la StackSet distribuzione.



Specificare StackSet i dettagli

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

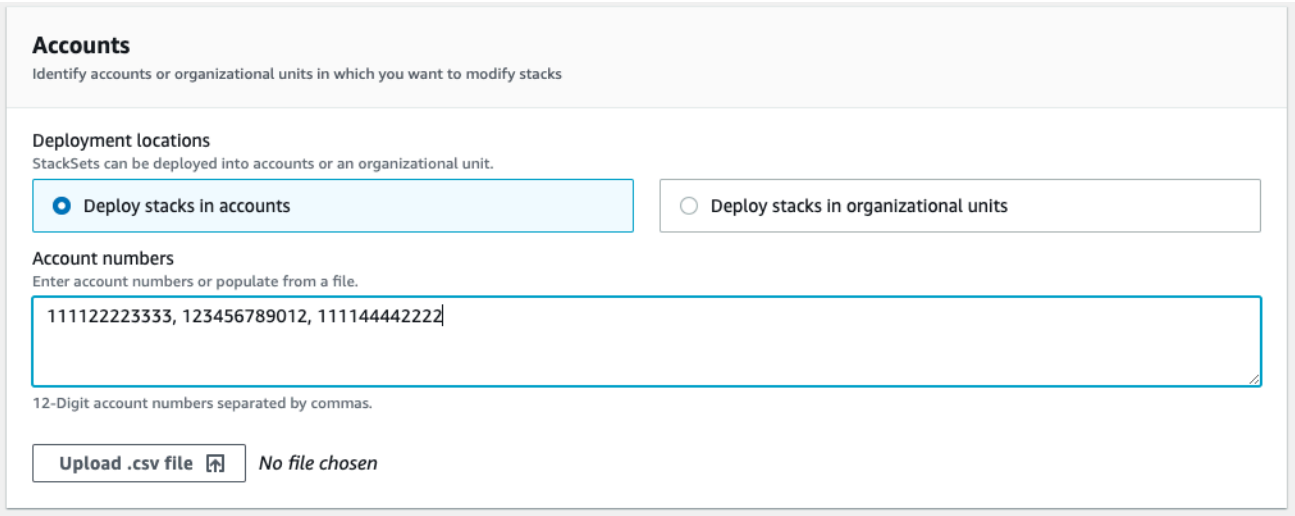
Poiché lo stack di membri utilizza stack annidati, è necessario implementarlo come sistema autogestito. StackSet Ciò non supporta la distribuzione automatica su nuovi account nell'organizzazione. AWS

Parametri

LogGroup Configurazione: scegli il gruppo di log che riceve CloudTrail i log. Se non ne esiste nessuno o se il gruppo di log è diverso per ogni account, scegli un valore conveniente. Gli amministratori degli account devono aggiornare il parametro Systems Manager — Parameter Store / Solutions/SO0111/Metrics _ LogGroupName dopo aver creato un gruppo di CloudWatch log per CloudTrail i registri. Questo è necessario per le riparazioni che creano allarmi metrici sulle chiamate. API

Standard: scegli gli standard da caricare nell'account del membro. Questa operazione installa solo i runbook di AWS Systems Manager e non abilita il Security Standard.

SecHubAdminAccount: Inserisci l'ID account dell'account AWS Security Hub Admin in cui hai installato il modello di amministrazione della soluzione.



Account

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

Specificare le regioni: seleziona tutte le regioni in cui desideri correggere i risultati. È possibile modificare le opzioni di distribuzione in base al numero di account e regioni. La concorrenza regionale può essere parallela.

Distribuzione automatizzata - Stacks

> **Note**
>
> Per i clienti con più account, consigliamo vivamente di implementare con. StackSets

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

Tempo di implementazione: circa 30 minuti

Prerequisiti

Prima di implementare questa soluzione, assicurati che AWS Security Hub si trovi nella stessa AWS regione degli account primario e secondario. Se hai già distribuito questa soluzione, devi disinstallare la soluzione esistente. Per ulteriori informazioni, consulta Aggiornare la soluzione.

Panoramica della distribuzione

Utilizza i seguenti passaggi per distribuire questa soluzione suAWS.

(Facoltativo) Fase 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 `aws-sharr-deploy.template` AWS CloudFormation modello nel tuo account AWS Security Hub amministratore.
- Scegli quali standard di sicurezza installare.
- Scegli un gruppo di log di Orchestrator esistente da utilizzare (seleziona `Yes` se esiste `SO0111-SHARR-Orchestrator` già da un'installazione precedente).

Fase 2: Installare i ruoli di riparazione in ogni account membro AWS Security Hub

- Avvia il `aws-sharr-member-roles.template` AWS CloudFormation modello in una regione per account membro.
- Inserisci l'account IG a 12 cifre per l'account AWS Security Hub amministratore.

Passaggio 3: avvia lo stack dei 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 log Logs che riceve CloudWatch i log. CloudTrail
- Scegli se installare i ruoli di riparazione. Installa questi ruoli solo una volta per account.
- Seleziona i playbook da installare.
- Inserisci l'ID dell'account AWS Security Hub amministratore.

Fase 4: (Facoltativo) Modifica le soluzioni correttive disponibili

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

(Facoltativo) Fase 0: Avvio di 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 oppure ServiceNow usali come modello per implementare la tua integrazione personalizzata.

   Per distribuire lo stack Jira:

   a. Inserisci un nome per lo stack.

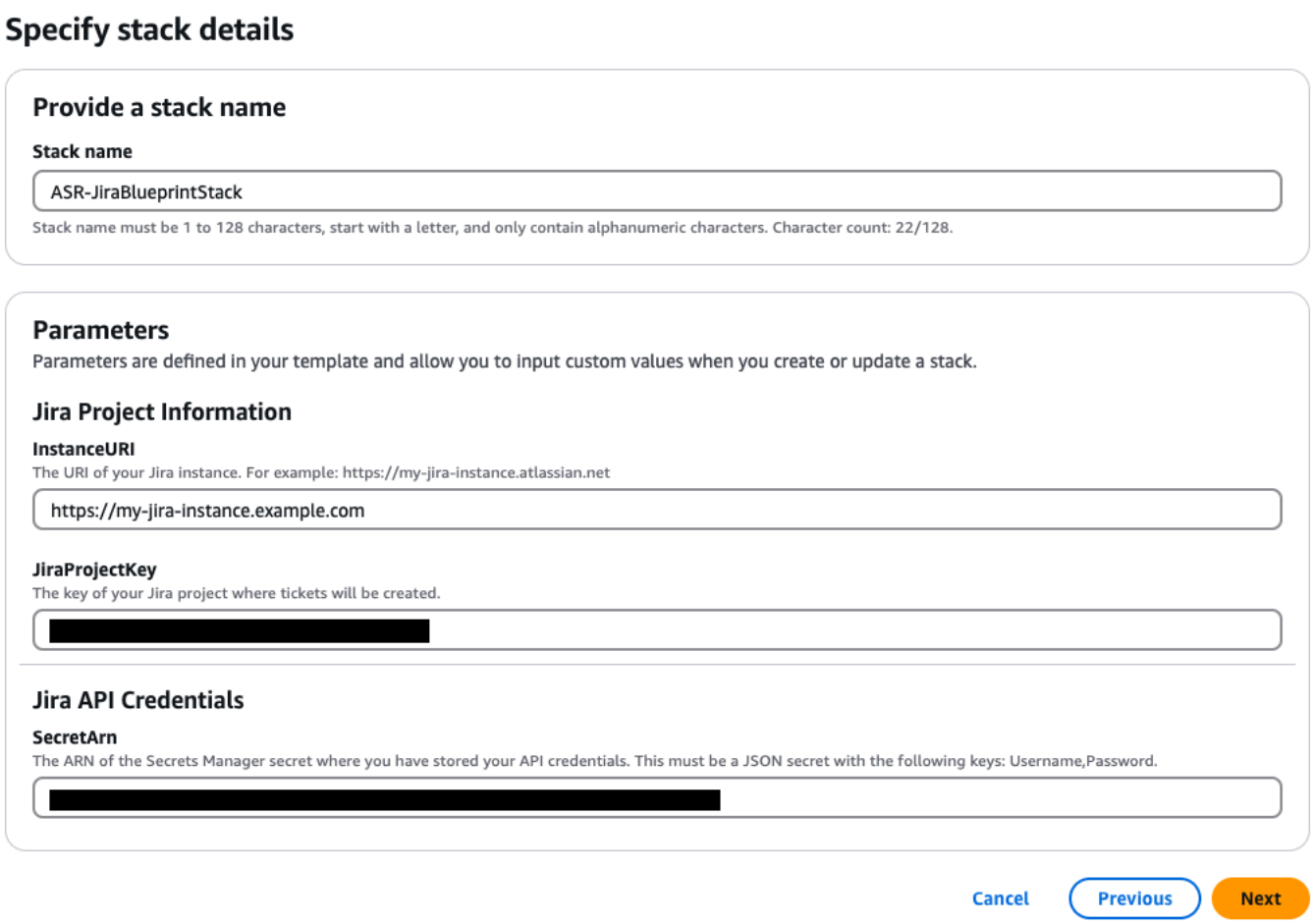
   b. Forniscilo URI alla tua istanza Jira.

   c. Fornisci la chiave del progetto Jira a cui desideri inviare i ticket.

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

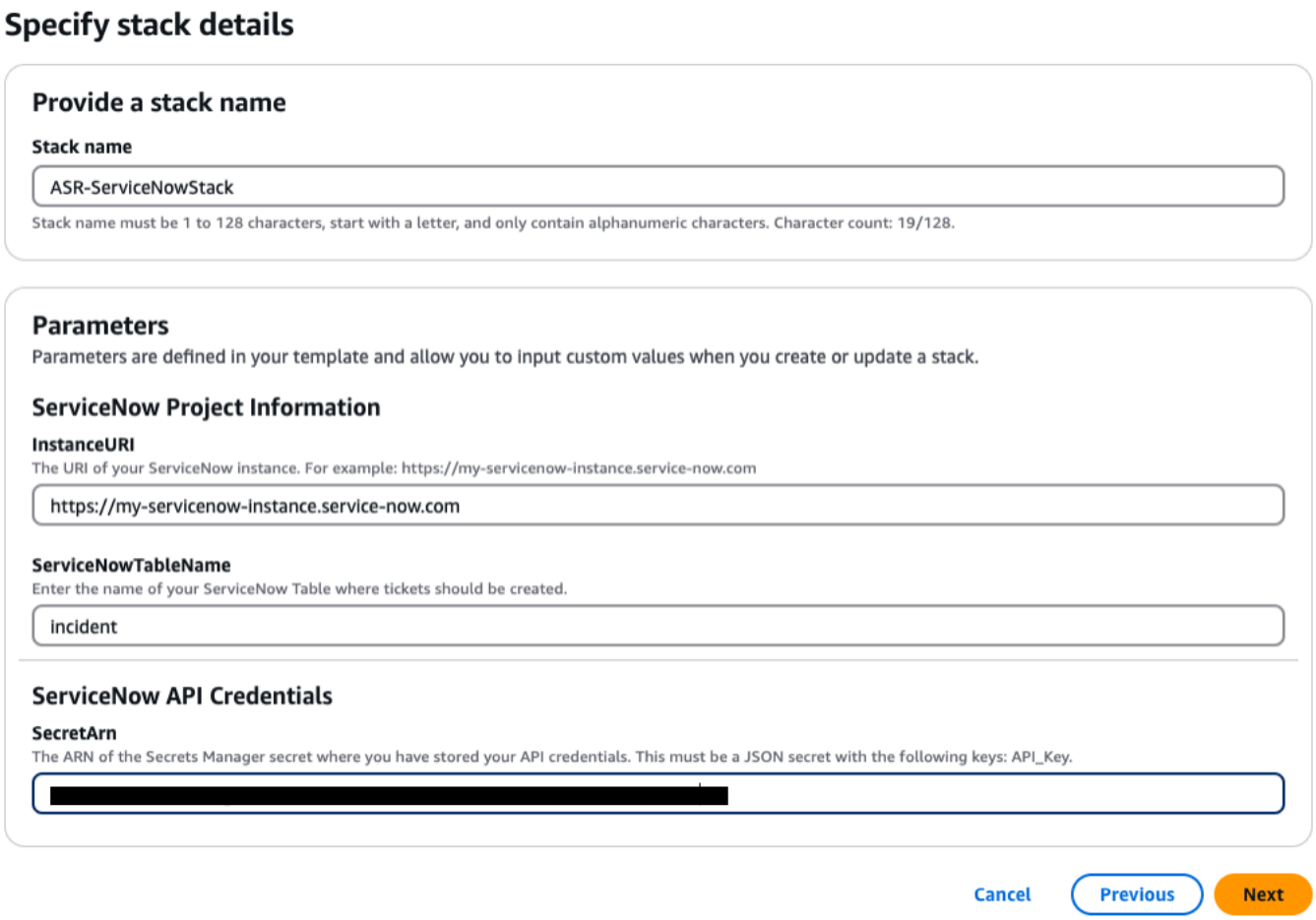
   > **Note**
   >
   > Puoi scegliere di utilizzare una API chiave Jira al posto della password fornendo il tuo nome utente come `Username` e la chiave come. API `Password`

   e. Aggiungi questo segreto come input allo stack. ARN



Per distribuire lo stack: ServiceNow

a. Inserisci un nome per lo stack.
b. Fornisci il nome URI della tua ServiceNow istanza.
c. Fornisci il nome della ServiceNow tabella.
d. Crea una API chiave ServiceNow con il permesso di modificare la tabella su cui intendi scrivere.
e. Crea un segreto in Secrets Manager con la chiave `API_Key` e fornisci il segreto ARN come input per lo stack.



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

Fase 1: Avvia lo stack di amministrazione

Important

Questa soluzione include un'opzione per inviare metriche operative anonime a. AWS Utilizziamo questi dati per comprendere meglio come i clienti utilizzano questa soluzione e i servizi e i prodotti correlati. AWSpossiede i dati raccolti tramite questo sondaggio. La raccolta dei dati è soggetta all'AWSInformativa sulla privacy.

Per disattivare questa funzionalità, scarica il modello, modifica la sezione di AWS CloudFormation mappatura, quindi utilizza la AWS CloudFormation console per caricare il

modello e distribuire la soluzione. Per ulteriori informazioni, consulta la sezione Raccolta di dati anonimi di questa guida.

Questo AWS CloudFormation modello automatizzato implementa l'Automated Security Response su una AWS soluzione nel cloud. AWS Prima di avviare lo stack, è necessario abilitare Security Hub e completare i prerequisiti.

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

1. Accedi AWS Management Console dall'account in cui AWS Security Hub è attualmente configurato e utilizza il pulsante in basso per avviare il `aws-sharr-deploy.template` AWS CloudFormation modello.

   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 un'altra AWS regione, utilizza il selettore della regione nella barra di navigazione. AWS Management Console

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

3. Nella pagina Create stack, verifica che il modello corretto URL sia nella casella di testo Amazon URL S3, quindi scegli Avanti.

4. Nella pagina Specificare i dettagli dello stack, assegna un nome allo stack di soluzioni. Per informazioni sulle limitazioni relative alla denominazione dei caratteri, consulta IAMe STS limiti nella Guida per l'utente.AWS Identity and Access Management
5. Nella pagina Parametri, scegli Avanti.

Parametro	Predefinito	Descrizione
Carica SC Admin Stack	`yes`	Specificate se installare i componenti di amministr azione per la riparazione automatica dei controlli SC.
Carica AFSBP Admin Stack	no	Specificate se installare i componenti di amministr azione per la riparazio ne automatica dei FSBP controlli.
Carica CIS12 0 Admin Stack	no	Specificate se installare i componenti di amministr azione per la riparazio ne automatica di CIS12 0 controlli.
Carica CIS14 0 Admin Stack	no	Specificate se installare i componenti di amministr azione per la riparazio ne automatica di CIS14 0 controlli.
Carica CIS3 00 Admin Stack	no	Specificare se installare i componenti di amministr azione per la riparazione automatica dei controlli CIS3 00.
Carica PC1321 Admin Stack	no	Specificate se installare i componenti di amministr

Parametro	Predefinito	Descrizione
		azione per la riparazione automatica dei PC1321 controlli.
Carica lo stack NIST di amministrazione	no	Specificate se installare i componenti di amministr azione per la riparazione automatica dei NIST controlli .
Riutilizza il gruppo di log di Orchestrator	no	Seleziona se riutilizzare o meno un gruppo di log esistente. `S00111-SH ARR-Orchestrator` CloudWatch Ciò semplific a la reinstallazione e gli aggiornamenti senza perdere i dati di registro di una versione precedente. Se stai eseguendo l'aggiorn amento dalla versione 1.2 o successiva, seleziona. `yes`
Usa le metriche CloudWatch	`yes`	Specificate se abilitare le CloudWatch metriche per il monitoraggio della soluzione. Questo creerà una CloudWatch dashboard per la visualizzazione delle metriche.

Parametro	Predefinito	Descrizione
Usa CloudWatch Metrics & Alarms	`yes`	Specificare se abilitare CloudWatch Metrics Alarms per la soluzione. Questo creerà allarmi per determina te metriche raccolte dalla soluzione.
RemediationFailure AlarmThreshold	5	Specificate la soglia per la percentuale di errori di riparazione per ID di controllo. Ad esempio, se si inserisce5, si riceve un allarme se un ID di controllo fallisce per più del 5% delle riparazioni in un determinato giorno. Questo parametro funziona solo se vengono creati allarmi (vedi il parametro Use CloudWatch Metrics Alarms).
EnableEnhancedClou dWatchMetrics	no	If`yes`, crea CloudWatch metriche aggiuntive per tenere traccia di tutti i controlli IDs singolarmente sulla CloudWatch dashboard e come allarmi. CloudWatch Consulta la sezione Costo per comprendere i costi aggiuntivi che ciò comporta.

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

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

Puoi visualizzare lo stato dello stack nella AWS CloudFormation console nella colonna Stato. Dovresti ricevere COMPLETE lo stato CREATE _ tra circa 15 minuti.

Fase 2: Installare i ruoli di riparazione in ogni account membro del AWS Security Hub

`aws-sharr-member-roles.template` StackSet Devono essere distribuiti in una sola regione per account membro. Definisce i ruoli globali che consentono le API chiamate tra account dalla funzione step di SHARR Orchestrator.

1. Accedi alla Console di AWS gestione per ogni account AWS Security Hub membro (incluso l'account amministratore, che è anche un membro). Seleziona il pulsante per avviare il `aws-sharr-member-roles.template` AWS CloudFormation modello. Puoi anche scaricare il modello come punto di partenza per un'implementazione personalizzata.

Launch solution

2. Per impostazione predefinita, il modello viene avviato nella regione Stati Uniti orientali (Virginia settentrionale). Per avviare questa soluzione in un'altra AWS regione, utilizza il selettore della regione nella barra di navigazione della console di AWS gestione.
3. Nella pagina Create stack, verifica che il modello corretto URL sia nella casella di testo Amazon URL S3, quindi scegli Avanti.
4. Nella pagina Specificare i dettagli dello stack, assegna un nome allo stack di soluzioni. Per informazioni sulle limitazioni relative ai nomi dei caratteri, consulta IAM e STS limiti nella AWS Identity and Access Management User Guide.
5. Nella pagina Parametri, specificate i seguenti parametri e scegliete Avanti.

Parametro	Predefinito	Descrizione
Spazio dei nomi	*<Requires input>*	Immettete una stringa composta da un massimo di 9 caratteri alfanumerici minuscoli. Questa stringa diventa parte dei nomi dei ruoli. IAM Utilizza lo stesso valore per la distribuzione dello stack dei membri e la distribuzione dello stack dei ruoli dei membri.
Amministratore dell'account Sec Hub	*<Requires input>*	Inserisci l'ID dell'account a 12 cifre per l'account AWS Security Hub amministratore. Questo valore concede le autorizzazioni per il ruolo di soluzione dell'account 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 per confermare che il modello creerà AWS Identity and Access Management () IAM risorse.
8. Seleziona Create (Crea) per implementare lo stack.

Puoi visualizzare lo stato dello stack nella AWS CloudFormation console nella colonna Stato. Dovresti ricevere COMPLETE lo stato CREATE _ tra circa 5 minuti. Puoi continuare con il passaggio successivo durante il caricamento di questo stack.

Passaggio 3: Avvia lo stack dei membri

> **Important**
>
> Questa soluzione include un'opzione per inviare metriche operative anonime a. AWS Utilizziamo questi dati per comprendere meglio come i clienti utilizzano questa soluzione e i servizi e i prodotti correlati. AWSpossiede i dati raccolti tramite questo sondaggio. La raccolta dei dati è soggetta all'AWSInformativa sulla privacy.
> Per disattivare questa funzionalità, scarica il modello, modifica la sezione di AWS CloudFormation mappatura, quindi utilizza la AWS CloudFormation console per caricare il modello e distribuire la soluzione. Per ulteriori informazioni, consulta la sezione Raccolta di metriche operative di questa guida.

Lo `aws-sharr-member` stack deve essere installato in ogni account membro del Security Hub. Questo stack definisce i runbook per la riparazione automatica. L'amministratore di ogni account membro può controllare quali rimedi sono disponibili tramite questo stack.

1. Accedi all'account AWS Management Console per ogni AWS Security Hub membro (incluso l'account amministratore, che è anche un membro). Seleziona il pulsante per avviare il `aws-sharr-member.template` AWS CloudFormation modello.

   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 un'altra AWS regione, utilizza il selettore della regione nella barra di navigazione. AWS Management Console

> **Note**
>
> Questa soluzione utilizza AWS Systems Manager, che è attualmente disponibile nella maggior parte delle AWS regioni. La soluzione funziona in tutte le regioni che supportano questi servizi. Per la disponibilità più aggiornata per regione, consulta l'Elenco dei servizi AWS regionali.

3. Nella pagina Create stack, verifica che il modello corretto URL sia nella casella di testo Amazon URL S3, quindi scegli Avanti.
4. Nella pagina Specificare i dettagli dello stack, assegna un nome allo stack di soluzioni. Per informazioni sulle limitazioni relative alla denominazione dei caratteri, consulta IAMe STS limiti nella Guida per l'utente.AWS Identity and Access Management
5. Nella pagina Parametri, specificate i seguenti parametri e scegliete Avanti.

Parametro	Predefinito	Descrizione
Fornisci il nome LogGroup da utilizzare per creare filtri e allarmi metrici	*<Requires input>*	Specificare il nome di un gruppo CloudWatch Logs in cui CloudTrail registra le chiamate. API Viene utilizzato per le riparazioni CIS 3.1-3.14.
Carica SC Member Stack	`yes`	Specificare se installare i componenti dei membri per la riparazione automatica dei controlli SC.
Carica lo stack AFSBP dei membri	no	Specificare se installare i componenti membri per la riparazione automatica dei FSBP controlli.
Carica CIS12 0 Member Stack	no	Specificare se installare i componenti membri per la

Parametro	Predefinito	Descrizione
		riparazione automatica di CIS12 0 controlli.
Carica lo stack di CIS14 0 membri	no	Specificare se installare i componenti membri per la riparazione automatica di CIS14 0 controlli.
Carica uno stack di CIS3 100 membri	no	Specificare se installare i componenti membri per la riparazione automatica dei controlli CIS3 00.
Carica lo stack PC1321 dei membri	no	Specificare se installare i componenti membri per la riparazione automatica dei PC1321 controlli.
Carica lo stack NIST dei membri	no	Specificare se installare i componenti membri per la riparazione automatica dei NIST controlli.
Crea un bucket S3 per la registrazione di audit di Redshift	no	Seleziona `yes` se il bucket S3 deve essere creato per la riparazione .4. FSBP RedShift Per i dettagli sul bucket S3 e sulla correzion e, consulta la correzione Redshift.4 nella Guida per l'utente.AWS Security Hub
Account amministratore Sec Hub	*<Requires input>*	Inserisci l'ID account a 12 cifre per l'account amministr atore AWS di Security Hub.

Parametro	Predefinito	Descrizione
Spazio dei nomi	*<Requires input>*	Inserisci una stringa composta da un massimo di 9 caratteri alfanumerici minuscoli. Questa stringa diventa parte dei nomi dei IAM ruoli e del bucket Action Log S3. Usa lo stesso valore per la distribuzione dello stack dei membri e la distribuzione dello stack dei ruoli dei membri. Questa stringa deve seguire le regole di denominazione di Amazon S3 per i bucket S3 generici.
EnableCloudTrailFo rASRActionLog	no	Seleziona `yes` se desideri monitorare gli eventi di gestione condotti dalla soluzione sulla dashboard . CloudWatch La soluzione crea una CloudTrail traccia in ogni account membro selezionato`yes`. Consulta la sezione Costo per comprendere i costi aggiuntiv i che ciò comporta.

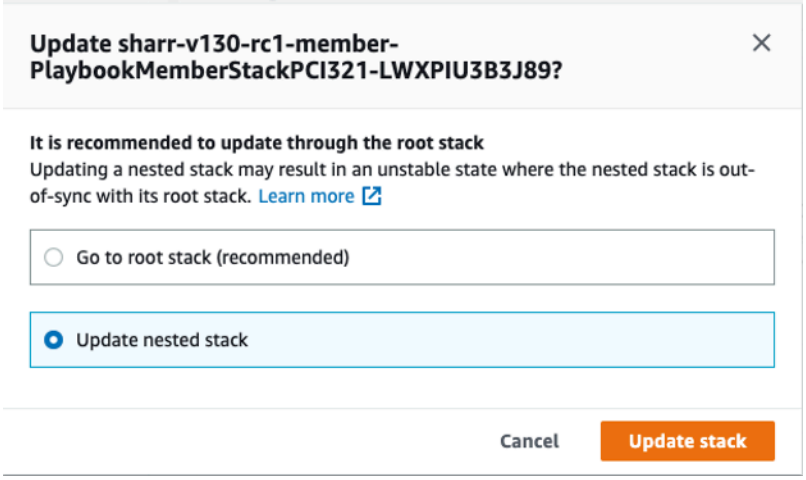
6. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
7. Nella pagina Rivedi, verifica e conferma le impostazioni. Seleziona la casella per confermare che il modello creerà AWS Identity and Access Management (IAM) risorse.
8. Seleziona Create (Crea) per implementare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

Puoi visualizzare lo stato dello stack nella AWS CloudFormation console nella colonna Stato. Dovresti ricevere COMPLETE lo stato CREATE _ tra circa 15 minuti.

Fase 4: (Facoltativo) Modifica le soluzioni correttive disponibili

Se desideri rimuovere rimedi specifici 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 AWS CloudFormation console e seleziona lo stack annidato.
2. Scegli Aggiorna.
3. Seleziona Aggiorna stack nidificato e scegli Aggiorna 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 i controlli indesiderati in. `Not available`

> **Note**
>
> La disattivazione di una correzione rimuove il runbook di correzione delle soluzioni 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 per confermare che il modello AWS Identity and Access Management creerà () risorse. IAM
8. Scegli Aggiorna stack.

Puoi visualizzare lo stato dello stack nella AWS CloudFormation console nella colonna Stato. Dovresti ricevere COMPLETE lo stato CREATE _ tra circa 15 minuti.

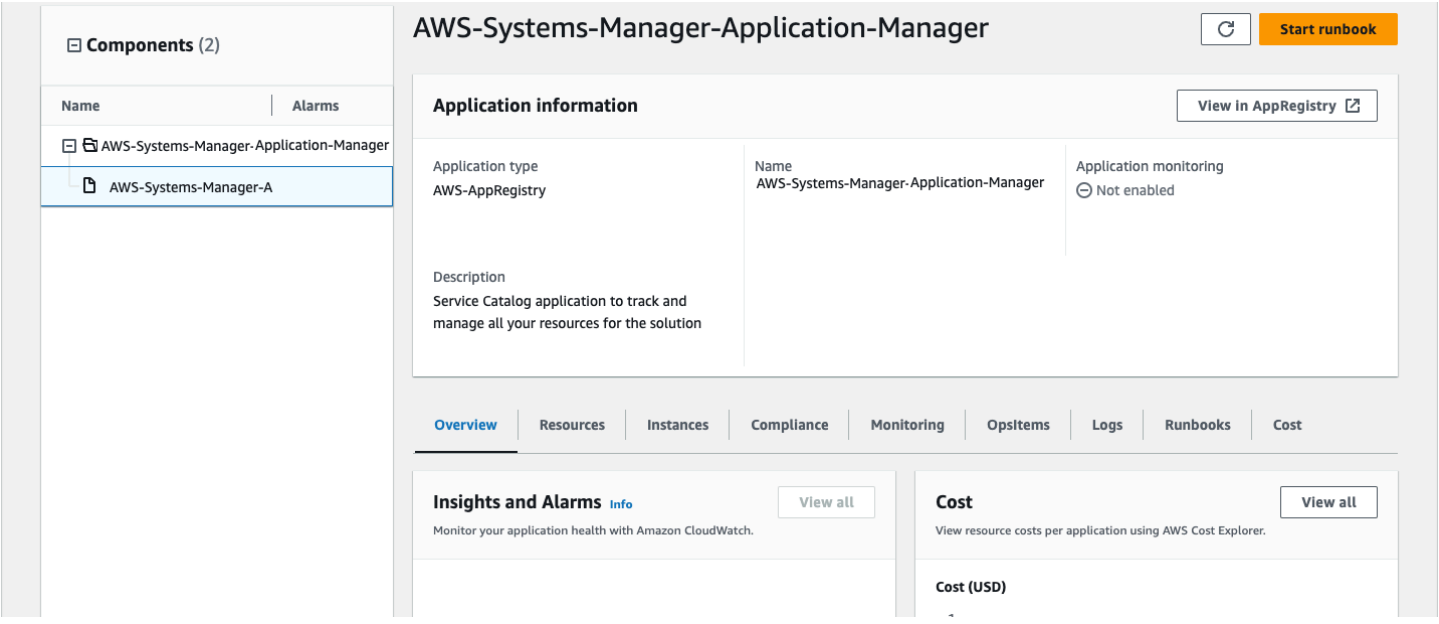
Monitora la soluzione con Service Catalog AppRegistry

Questa soluzione include una AppRegistry risorsa Service Catalog per registrare il CloudFormation modello e le risorse sottostanti come applicazione sia in Service Catalog AppRegistry che in AWS Systems Manager Application Manager.

AWS Systems Manager Application Manager offre una visione a livello di applicazione di questa soluzione e delle relative risorse in modo da poter:

- Monitora le risorse, i costi delle risorse distribuite tra gli stack e Account AWS i log associati a questa soluzione da una posizione centrale.
- Visualizza i dati operativi relativi alle risorse di questa soluzione (come lo stato dell'implementazione, gli CloudWatch allarmi, le configurazioni delle risorse e i problemi operativi) nel contesto di un'applicazione.

  La figura seguente mostra un esempio di visualizzazione delle applicazioni per lo stack di soluzioni in Application Manager.



Stack di soluzioni in Application Manager

Usa CloudWatch Application Insights

Questa soluzione si integra automaticamente con CloudWatch Application Insights al momento dell'implementazione. CloudWatch Application Insights ti aiuta a vedere e comprendere lo stato di salute e le prestazioni della soluzione mediante:

- Individuazione e monitoraggio automatici delle risorse principali delle applicazioni.
- Creazione di allarmi personalizzati per identificare in modo proattivo potenziali problemi.
- Generazione automatica di Systems Manager OpsItems quando vengono rilevate anomalie o guasti. Queste OpsItems servono come notifiche utilizzabili che informano tempestivamente l'utente dei problemi che influiscono sulla soluzione.

Segui questi passaggi per visualizzare la dashboard di monitoraggio di CloudWatch Application Insights, dove puoi visualizzare lo stato della soluzione e monitorare i componenti chiave tramite dashboard e allarmi preconfigurati.

1. Passare alla console CloudWatch .
2. Scegli la scheda Insights e seleziona Application Insights.
3. Scegli la scheda Applicazioni, quindi seleziona l'applicazione associata alla soluzione.

Puoi anche importare la CloudWatch dashboard della soluzione per consolidare il monitoraggio dello stato della soluzione. Nella dashboard dell'applicazione della soluzione in CloudWatch Application Insights, segui questi passaggi:

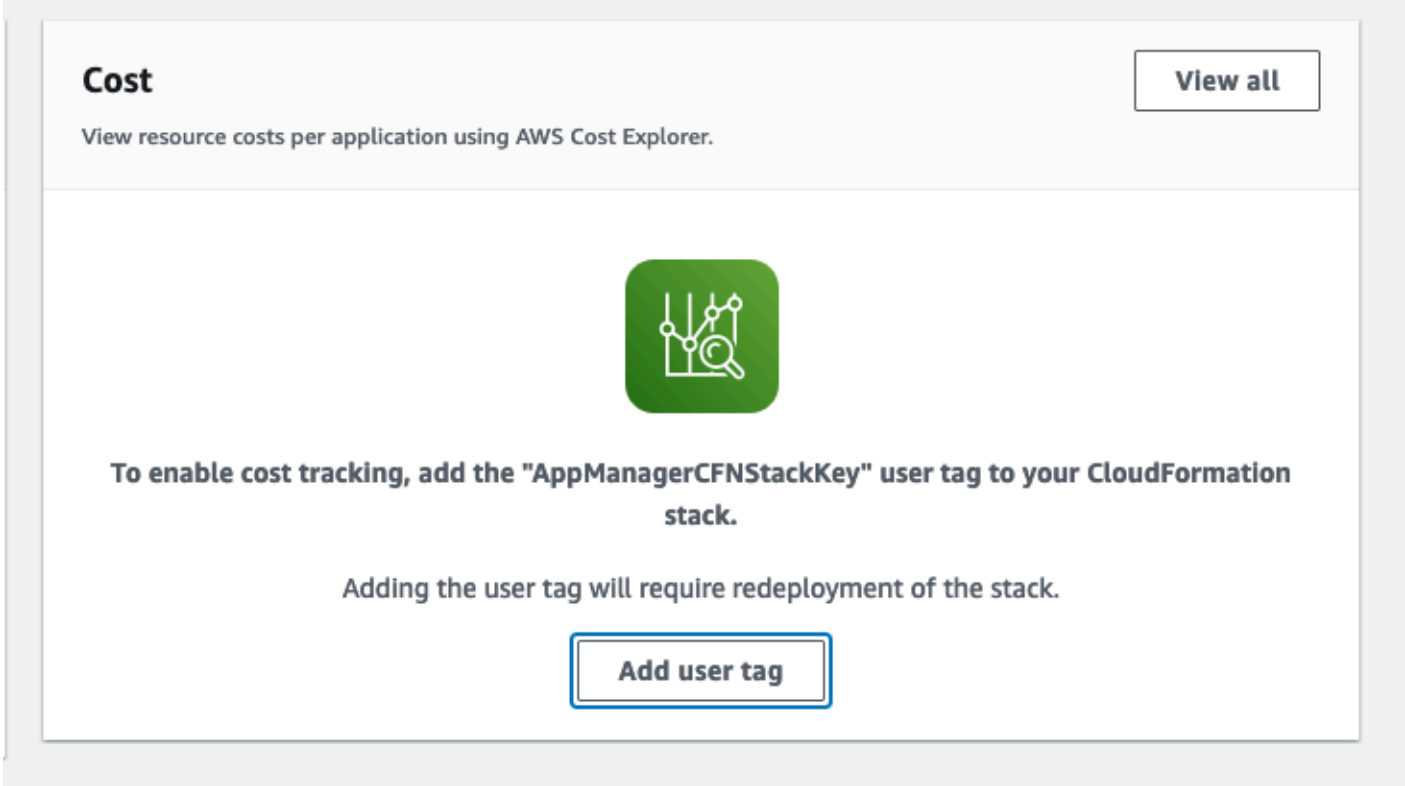
1. Scegli la scheda CloudWatch Dashboard personalizzata.
2. Scegli Importa CloudWatch dashboard.
3. Nella casella di ricercaASR-Remediation-Metrics-Dashboard, inserisci e seleziona Automated Security Response sulla AWS dashboard.
4. Seleziona Importa.

Ora puoi visualizzare la dashboard di CloudWatch Application Insights e la dashboard personalizzata della soluzione entrambe all'interno della console di CloudWatch Application Insights, senza dover passare da una pagina all'altra.

Conferma i cartellini dei costi associati alla soluzione

Dopo aver attivato i tag di allocazione dei costi associati alla soluzione, è necessario confermare i tag di allocazione dei costi per visualizzare i costi di questa soluzione. Per confermare i tag di allocazione dei costi:

1. Accedere alla console Systems Manager.
2. Nel riquadro di navigazione, scegli Application Manager.
3. In Applicazioni, scegli il nome dell'applicazione per questa soluzione e selezionala.
4. Nella scheda Panoramica, in Costo, seleziona Aggiungi tag utente.



5. Nella pagina Aggiungi tag utente, inserisci`confirm`, quindi seleziona Aggiungi tag utente.

Il completamento del processo di attivazione può richiedere fino a 24 ore e la visualizzazione dei dati del tag.

Attiva i tag di allocazione dei costi associati alla soluzione

Dopo aver confermato i tag dei costi associati a questa soluzione, è necessario attivare i tag di allocazione dei costi per visualizzare i costi di questa soluzione. I tag di allocazione dei costi possono essere attivati solo dall'account di gestione dell'organizzazione.

Per attivare i tag di allocazione dei costi:

1. Accedi alla console AWS Billing and Cost Management and Cost Management.
2. Nel riquadro di navigazione, seleziona Tag di allocazione dei costi.
3. Nella pagina Tag di allocazione dei costi, filtra il `AppManagerCFNStackKey` tag, quindi seleziona il tag dai risultati visualizzati.
4. Seleziona Activate (Attiva).

AWS Cost Explorer

È possibile visualizzare la panoramica dei costi associati all'applicazione e ai componenti dell'applicazione all'interno della console di Application Manager tramite l'integrazione con AWS Cost Explorer. Cost Explorer ti aiuta a gestire i costi fornendo una panoramica dei costi e dell'utilizzo AWS delle risorse nel tempo.

1. Accedi alla console di gestione dei AWS costi.
2. Nel menu di navigazione, seleziona Cost Explorer per visualizzare i costi e l'utilizzo della soluzione nel tempo.

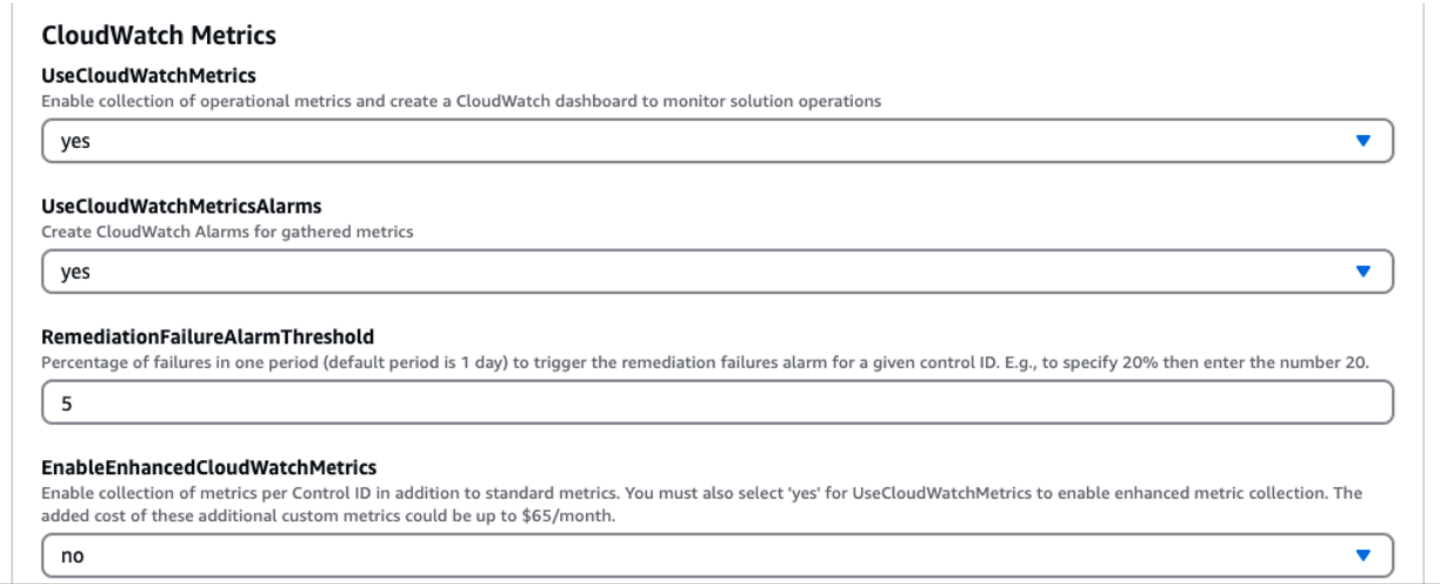
Monitora le operazioni della soluzione con una CloudWatch dashboard Amazon

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

La CloudWatch dashboard e gli allarmi monitorano le operazioni della soluzione e avvisano quando c'è un potenziale problema.

Abilitazione di CloudWatch metriche, allarmi e dashboard

Esistono quattro parametri del CloudFormation modello per la CloudWatch funzionalità.



1. UseCloudWatchMetrics— Questa impostazione `yes` consente la raccolta di metriche operative e crea una CloudWatch dashboard per visualizzare tali metriche.
2. UseCloudWatchAlarms— Impostazione per `yes` abilitare gli allarmi predefiniti della soluzione.
3. RemediationFailureAlarmThreshold— La percentuale di riparazioni non riuscite in un periodo in cui viene generato un allarme.
4. EnableEnhancedCloudWatchMetrics— Imposta questo parametro per `yes` raccogliere metriche individuali per ID di controllo. Per impostazione predefinita, questo parametro è impostato suno, in modo che vengano raccolte solo le metriche relative al numero totale di correzioni relative a tutto il controlloIDs. Le metriche e gli allarmi individuali per ID di controllo comportano costi aggiuntivi.

Utilizzo della dashboard CloudWatch

Per visualizzare la dashboard:

1. Vai su Amazon CloudWatch e poi su Dashboards.
2. Seleziona la dashboard denominata "ASR-Remediation-Metrics-Dashboard».

La dashboard contiene le seguenti sezioni: CloudWatch

1. Rimediazioni riuscite totali: fornisce informazioni sul numero di risultati del Security Hub che sono stati risolti con successo dalla soluzione.
2. Risoluzioni non riuscite: mostra quante riparazioni non sono riuscite, in totale e in percentuale, e la causa dell'errore. Un numero elevato di errori può suggerire la presenza di un problema tecnico relativo alla soluzione che potrebbe essere necessario esaminare in modo più dettagliato.
3. Riparazione successa/fallimento per Control ID: se hai abilitato Enhanced Metrics al momento della distribuzione, questa sezione elenca i risultati della correzione per ID di controllo. Quando la sezione Errori di riparazione mostra un tasso di errore elevato in generale, in questa sezione viene indicato se gli errori sono distribuiti su più controlli o se solo alcuni controlli IDs falliscono. IDs
4. Runbook Assume Role Failures: mostra il numero di errori che si sono verificati a causa di tentativi di riparazione in account in cui non è installato il ruolo Solution Member. I ripetuti errori dovuti ai tentativi di riparazione automatici dovuti alla mancanza di ruoli causano costi inutili. Attenua 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 su tutti gli account membro in cui hai abilitato Action Logs con il parametro al momento dell'implementazione. EnableCloudTrailForASRActionLog Quando osservi cambiamenti imprevisti delle risorse in uno qualsiasi dei tuoi AWS account, questo widget può aiutarti a capire se le risorse sono state modificate dalla soluzione.

La CloudWatch dashboard è inoltre dotata di allarmi predefiniti che avvisano degli errori operativi più comuni.

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

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

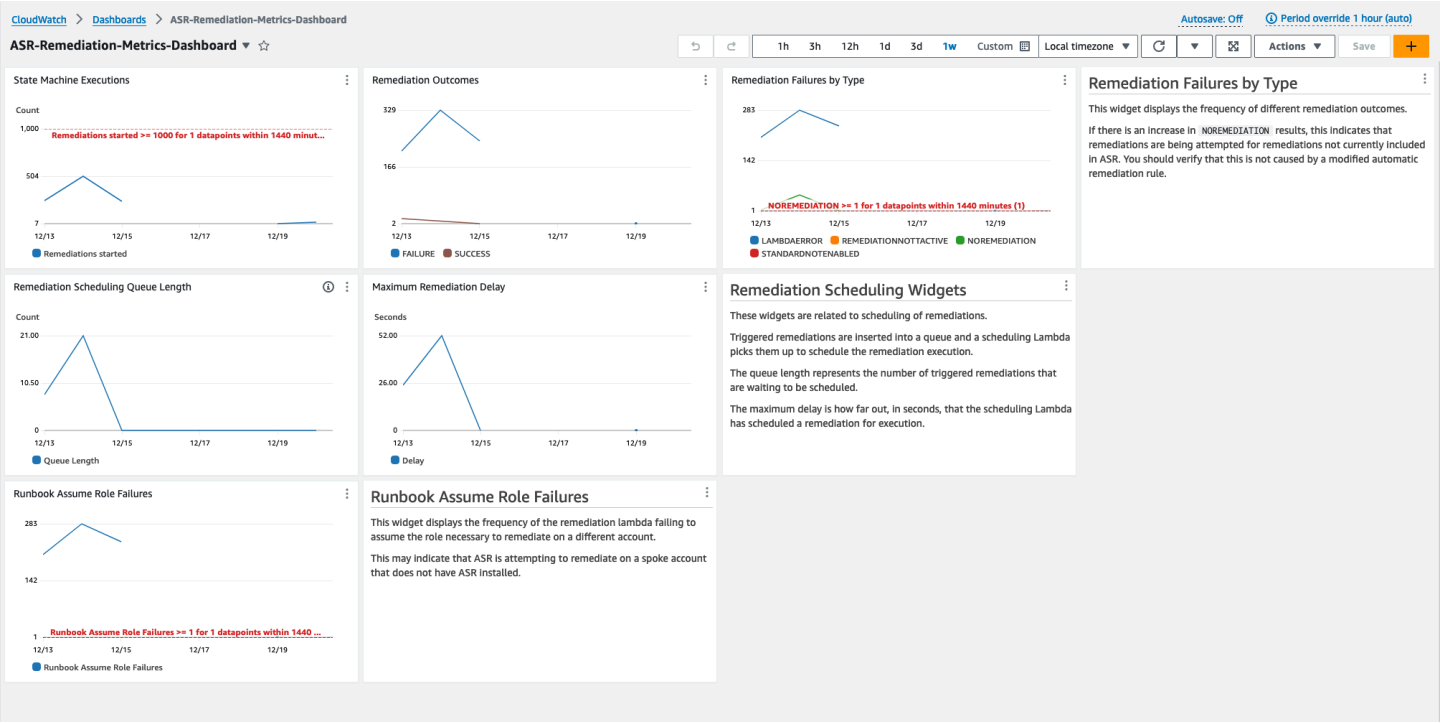
2. Errori di riparazione per tipo = > 0 NOREMEDIATION

   a. Sono in corso tentativi di riparazione per riparazioni non incluse in. ASR Ciò potrebbe indicare che una regola di evento è stata modificata per includere più riparazioni rispetto a quelle previste.

3. Runbook Assume errori di ruolo > 0

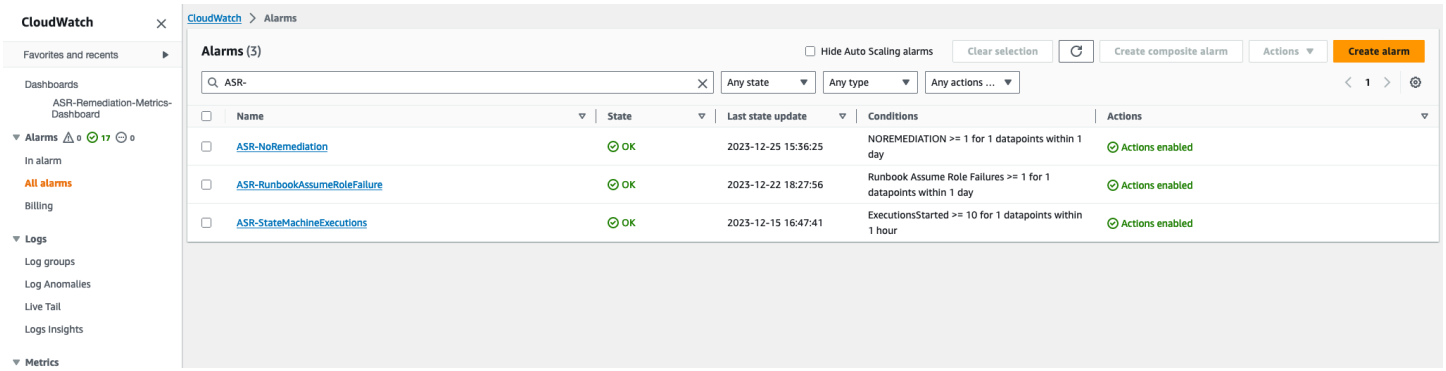
   a. Sono in corso tentativi di riparazione su account o regioni in cui la soluzione non è stata distribuita correttamente. Ciò potrebbe indicare che una regola relativa all'evento è stata modificata per includere più account del previsto.

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

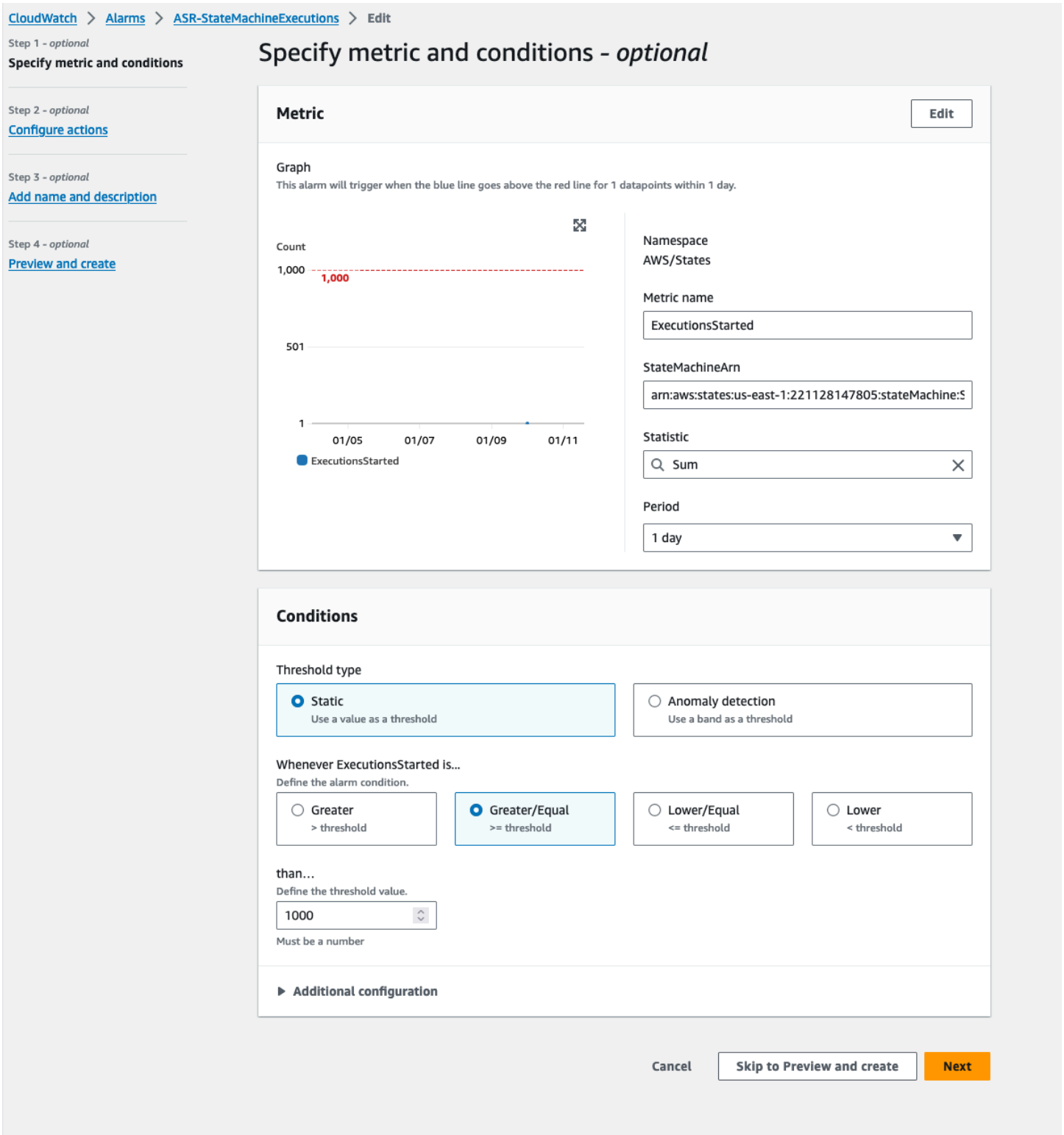


Modifica delle soglie di allarme

1. Vai su Amazon CloudWatch -> Allarmi -> Tutti gli allarmi.
2. Scegli l'allarme che desideri modificare, quindi seleziona Azioni -> Modifica.



3. Modifica la soglia con il valore desiderato e salva.



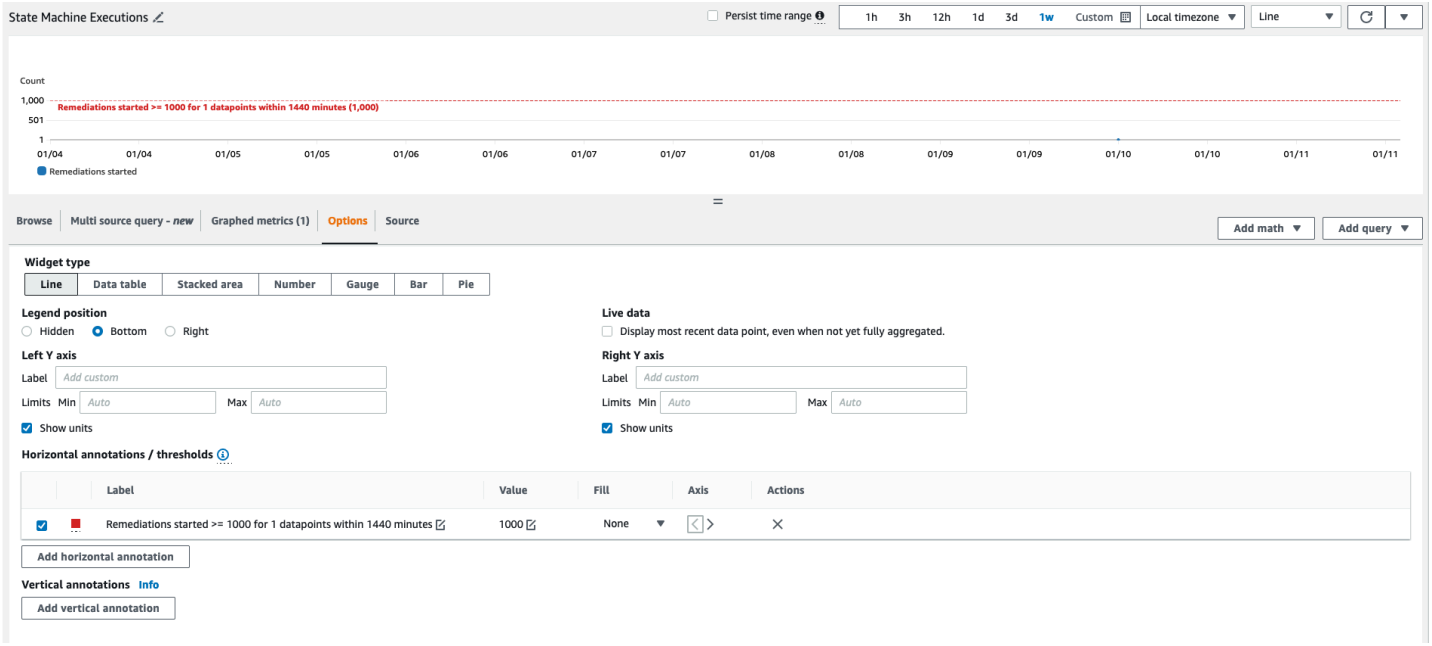
4. Vai alla CloudWatch dashboard per modificare i grafici in modo che corrispondano alle nuove impostazioni.

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

b. Seleziona Edit (Modifica).

c. Passate alla scheda Opzioni.

d. Modifica l'annotazione dell'allarme in modo che corrisponda alle nuove impostazioni.



Iscrizione alle notifiche di allarme

Nell'account amministratore, iscriviti all'SNSargomento Amazon creato dallo stack di amministrazione, SO0111- _Alarm_Topic. ASR Questo ti avviserà quando entra in funzione un allarme. ALARM

Aggiorna la soluzione

Aggiornamento da versioni precedenti alla v1.4

Se hai già distribuito la soluzione prima della versione 1.4.x, disinstallala e installa la versione più recente:

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

> **Note**
>
> Se stai effettuando l'aggiornamento dalla v1.2.1 o precedente alla v1.3.0 o successiva, imposta Use existing Orchestrator Log Group su. No Se stai reinstallando la versione 1.3.0 o successiva, puoi selezionare questa opzione. `Yes` Questa opzione consente di continuare a accedere allo stesso gruppo di log per Orchestrator Step Functions.

Aggiornamento dalla v1.4 e versioni successive

Se stai eseguendo 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.
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 utilizzando il modello più recente.

Aggiornamento dalla v2.0.x

Se stai effettuando l'aggiornamento dalla v2.0.x, esegui l'aggiornamento alla versione 2.1.2 o successiva. L'aggiornamento alla v2.1.0 - v2.1.1 avrà esito negativo. CloudFormation

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 le istruzioni per aprire una AWS richiesta di assistenza per questa soluzione.

Registri delle soluzioni

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

Questa soluzione raccoglie l'output dai runbook di correzione, che vengono eseguiti sotto AWS Systems Manager, e registra il risultato nel gruppo CloudWatch `S00111-SHARR` Logs dell'account amministratore. AWS Security Hub C'è un solo stream per controllo al giorno.

Orchestrator Step Functions registra tutte le transizioni di passaggio nel gruppo `S00111-SHARR-Orchestrator` CloudWatch Logs nell'account amministratore di Security Hub. AWS Questo registro è una traccia di controllo per registrare le transizioni di stato per ogni istanza di Step Functions. Esiste un flusso di log per ogni esecuzione di Step Functions.

Entrambi i gruppi di log sono crittografati utilizzando una chiave AWS KMS Customer-Manager ()CMK.

Le seguenti informazioni per la risoluzione dei problemi utilizzano il gruppo di `S00111-SHARR` log. Utilizza questo registro, oltre alla console AWS Systems Manager Automation, ai registri di Automation Executions, alla console Step Function e ai registri Lambda per risolvere i problemi.

Se una riparazione fallisce, nel flusso di log verrà registrato un messaggio simile al seguente `S00111-SHARR` nel flusso di log per lo standard, il controllo e la data. Ad esempio: -2.9-2021-08-12 CIS

```
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 output proviene dal SHARR runbook per lo standard di sicurezza e il controllo. Ad esempio: SHARR- CIS _1.2.0_2.9

```
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 del membro. Per risolvere questo problema, è necessario accedere all'account del membro (indicato AWS Management Console nel messaggio precedente), accedere a AWS Systems ManagerAutomation ed esaminare l'output del registro relativo all'ID di esecuzione. `eecdef79-9111-4532-921a-e098549f525`

Risoluzione di problemi noti

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

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

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

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

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

  Soluzione: distribuisci lo stack di amministrazione nello stesso account e nella stessa regione dell'amministratore del 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- SHARR -Orchestrator non funziona nello stato del documento Get Automation con un errore 502: «Lambda non è riuscita a decrittografare le variabili di ambiente perché l'accesso è stato negato. KMS Controlla KMS le impostazioni dei tasti della funzione. KMS Eccezione: UnrecognizedClientException KMS Messaggio: il token di

sicurezza incluso nella richiesta non è valido. (Servizio: AWSLambda; Codice di stato: 502; Codice di errore:KMSAccessDeniedException; ID richiesta:...»

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

- Problema: ho cercato di porre rimedio a un problema ma non è successo nulla.

  Risoluzione: controlla le note del risultato per scoprire i motivi per cui non è stato corretto. Una causa comune è che non è prevista alcuna correzione automatica del problema. Al momento non è possibile fornire un feedback diretto all'utente se non esiste alcuna soluzione se non tramite le note. Esamina i log della soluzione. Apri CloudWatch Logs nella console. Trova il gruppo SO0111- Logs. SHARR CloudWatch Ordina l'elenco in modo che gli stream aggiornati più di recente vengano visualizzati per primi. Seleziona il flusso di registro per il risultato che hai tentato di eseguire. Dovresti trovare eventuali errori lì. Alcune ragioni dell'errore potrebbero essere: mancata corrispondenza tra Finding Control e Correation Control, risoluzione tra account diversi (non ancora supportata) o il fatto che il risultato sia già stato risolto. Se non riesci a determinare il motivo dell'errore, raccogli i log e apri un ticket di assistenza.
- Problema: dopo aver avviato una riparazione, lo stato nella console 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 Failed a Passed. I risultati vengono creati dai dati degli eventi inviati da altri servizi, come AWS Config, a AWS Security Hub. Il tempo prima che una regola venga rivalutata dipende dal servizio sottostante. Se ciò non risolve il problema, consulta la risoluzione precedente dicendo «Ho tentato di correggere un problema ma non è successo nulla».
- Problema: la funzione step di Orchestrator non funziona 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 su cui si SHARR sta tentando di correggere un risultato. Segui le istruzioni per la distribuzione del modello di membro.
- Problema: il runbook Config.1 non funziona perché il registratore o il canale di distribuzione esistono già.

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

- 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 correzione non restituiscono una risposta. I runbook di correzione falliranno correttamente e segnaleranno la soluzione se non funzionano.

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

  Risoluzione: a volte perdiamo l'opportunità di gestire una condizione di errore che genera una traccia dello stack anziché un messaggio di errore. Tentativo di risolvere il problema utilizzando i dati di traccia. 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 a seguito della rimozione dell'azione personalizzata. Si tratta di un problema noto che verrà risolto nella prossima versione. Se ciò si verifica:

  1. Accedi alla console di gestione AWS di Security Hub.
  2. Nell'account amministratore, vai a Impostazioni.
  3. Seleziona la scheda Azioni personalizzate
  4. Eliminare manualmente la voce Rimedia con SHARR.
  5. Elimina nuovamente lo stack.

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

  Soluzione: 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 dei membri. È necessario ridistribuire lo stack dei ruoli dei membri in tutti gli account dei membri.

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

  Soluzione: si tratta di un evento comune se non hai sottoscrizioni all'`SO0111-SHARR_LocalAlarmNotification`SNSargomento nell'account del membro.

Problemi con correzioni specifiche

S etSSLBucket Policy fallisce con AccessDenied errori

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

Problema: etSSLBucket la politica S AccessDenied fallisce con un errore:

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

Se l'impostazione Block Public Access è stata abilitata per un bucket, i tentativi di inserire una policy bucket che includa istruzioni che consentono l'accesso pubblico falliscono con questo errore. Questo stato può essere raggiunto inserendo una policy bucket che contenga tali istruzioni e quindi abilitando il blocco dell'accesso pubblico per quel bucket.

La correzione ConfigureS3 BucketPublicAccessBlock (controlli associati: AWS FSBP v1.0.0 S3.2, PCI v3.2.1 PCI .S3.2, CIS v1.4.0 2.1.5.2, SC v2.0.0 S3.2) può anche impostare un bucket in questo stato perché imposta l'impostazione del blocco di accesso pubblico senza modificare la politica del bucket.

La etSSLBucket politica S aggiunge una dichiarazione alla policy del bucket per SSL rifiutare le richieste che non vengono utilizzate. Non modifica le altre istruzioni della policy, quindi se ci sono istruzioni che consentono l'accesso pubblico, la correzione fallirà nel tentativo di inserire la policy bucket modificata che include ancora tali istruzioni.

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

PutS3 fallisce BucketPolicyDeny

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

Problema: il BucketPolicyDeny putS3 con il seguente errore:

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

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

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

Come disattivare la soluzione

In caso di incidente, potrebbe essere necessario disabilitare la soluzione senza rimuovere alcuna infrastruttura. Questi scenari descrivono in dettaglio come disattivare diversi componenti della soluzione.

Scenario 1: disabilita la riparazione automatica per un singolo controllo.

1. Accedere EventBridge alla AWS CloudFormation console.
2. Seleziona Regole nella barra laterale.
3. Seleziona il bus degli eventi predefinito e cerca il controllo che desideri disabilitare.
4. Seleziona la regola e seleziona il pulsante Disabilita.

Scenario 2: disabilita la riparazione automatica per tutti i controlli.

1. Accedere EventBridge alla console.
2. Seleziona Regole nella barra laterale.
3. Seleziona il bus degli eventi «predefinito» e seleziona tutte le regole di seguito.
4. Seleziona il pulsante «Disabilita». Tieni presente che potrebbe essere necessario eseguire questa operazione per più pagine di regole.

Scenario 3: disabilita la riparazione manuale per un account

1. Vai a EventBridge nella console.
2. Seleziona Regole nella barra laterale.
3. Seleziona il bus degli eventi «predefinito» e cerca «SHARRRemediate_with_ _» CustomAction
4. Seleziona la regola e seleziona il pulsante «Disabilita».

Contatto Support

Se disponi di AWSDeveloper Support, AWS Business Support o AWSEnterprise Support, puoi utilizzare il Support Center per ottenere l'assistenza di esperti su questa soluzione. Le istruzioni per eseguire tali operazioni sono fornite nelle sezioni seguenti.

Crea un caso

1. Accedi al Support Center.
2. Scegli Crea caso.

Come possiamo aiutarti?

1. Scegli Tecnico.
2. Per Assistenza, seleziona Soluzioni.
3. Per Categoria, seleziona Altre soluzioni.
4. Per Severità, seleziona l'opzione più adatta al tuo caso d'uso.
5. Quando si inseriscono i campi Servizio, Categoria e Severità, l'interfaccia compila 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. In Oggetto, inserisci il testo che riassume la domanda o il problema.
2. Per Descrizione, descrivi il problema in dettaglio.
3. Scegli Allega file.
4. Allega le informazioni Support necessarie 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 subito o contattaci

1. Rivedi 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

Utilizzare la procedura seguente per disinstallare la soluzione con AWS Management Console.

V1.0.0-V1.2.1

Per le versioni da v1.0.0 a v1.2.1, usa Service Catalog per disinstallare e/o Playbook. CIS FSBP Con la v1.3.0 Service Catalog non viene più utilizzato.

1. Accedi alla AWS CloudFormation console e vai all'account principale di Security Hub.
2. Scegli Service Catalog per chiudere tutti i playbook forniti, rimuovere gruppi, ruoli o utenti di sicurezza.
3. Rimuovi il `CISPermissions.template` modello spoke dagli account dei membri del Security Hub.
4. Rimuovi il `AFSBPMemberStack.template` modello spoke dagli account amministratore e membro di Security Hub.
5. Passa all'account principale di Security Hub, seleziona lo stack di installazione della soluzione, quindi scegli Elimina.

> **Note**
>
> CloudWatch Registri I registri di gruppo vengono conservati. Si consiglia di conservare questi registri come richiesto dalla politica di conservazione dei log dell'organizzazione.

V1.3.x

1. Rimuovi il `aws-sharr-member.template` da ogni account membro.
2. Rimuovi il `aws-sharr-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. Utilizza le seguenti istruzioni per risolvere il problema:

1. Accedi alla console di gestione AWS di Security Hub.
2. Nell'account amministratore, vai a Impostazioni.
3. Seleziona la scheda Azioni personalizzate.
4. Eliminare manualmente la voce Rimedia con SHARR.
5. Elimina nuovamente lo stack.

V1.4.0 e versioni successive

Implementazione dello stack

1. Rimuovi il `aws-sharr-member.template` da ogni account membro.
2. Rimuovi il `aws-sharr-admin.template` dall'account amministratore.

StackSet distribuzione

Per ciascuna di esse StackSet, rimuovi le pile, quindi rimuovile StackSet nell'ordine inverso rispetto alla distribuzione.

Tieni presente che IAM i ruoli di `aws-sharr-member-roles.template` vengono mantenuti anche se il modello viene rimosso. In questo modo le riparazioni che utilizzano questi ruoli continueranno a funzionare. Questi ruoli SO0111-* possono essere rimossi manualmente dopo aver verificato che non siano più utilizzati mediante correzioni attive, ad esempio alla registrazione o al monitoraggio avanzato. CloudTrail CloudWatch RDS

Guida per amministratori

Abilitazione e disabilitazione di parti della soluzione

In qualità di amministratore della soluzione, hai i seguenti controlli su quali funzionalità della soluzione sono abilitate.

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

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

Configurazione dell'aggregazione di ricerca dell'account e della regione in Security Hub:

- Lo stack di amministrazione sarà in grado di avviare correzioni (tramite azioni personalizzate o EventBridge regole completamente automatizzate) solo per i risultati che arrivano nell'account di amministrazione e nella regione.
- Per esonerare completamente gli account o le regioni dal controllo della soluzione, non includere 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 implementati:

- Lo stack di amministrazione sarà in grado di avviare correzioni (tramite azioni personalizzate o EventBridge regole completamente automatizzate) solo per i controlli che hanno un runbook di controllo distribuito nell'account membro e nella regione di destinazione. Questi vengono implementati dallo stack di membri per ogni standard.
- Lo stack di amministrazione sarà in grado di avviare riparazioni completamente automatizzate solo utilizzando EventBridge regole per i controlli che hanno le regole implementate dallo stack di amministrazione per quello standard. Queste vengono distribuite all'account amministratore.
- Per semplicità, consigliamo di implementare gli standard in modo coerente tra gli account amministratore e membro. Se ti interessa AWS FSBP la CIS versione 1.2.0, distribuisci questi due

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

Quali runbook di Control vengono distribuiti in ogni stack di membri nidificato:

- Lo stack di amministrazione sarà in grado di avviare correzioni (tramite azioni personalizzate o EventBridge regole completamente automatizzate) solo per i controlli che hanno un runbook di controllo distribuito nell'account membro e nella regione di destinazione dallo stack membro per ogni standard.
- Per esercitare un controllo più preciso sui controlli abilitati per un particolare standard, ogni stack annidato per uno standard contiene parametri per i quali vengono distribuiti i control runbook. Imposta il parametro per un controllo sul valore «NOTAvailable» per annullare la distribuzione di quel runbook di controllo.

SSMParametri per abilitare e disabilitare gli standard:

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

Notifiche di esempio 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 successo

```
{
  "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"
  }
}
```

Usa la soluzione

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

Tutorial: Guida introduttiva a Automated Security Response 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 trovati in un account membro.

Prepara i conti

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

Negli esempi seguenti vengono utilizzati gli account `111111111111` e `222222222222` viene illustrata la soluzione. `111111111111`sarà l'account amministratore e `222222222222` sarà l'account membro. Definiremo la soluzione per correggere 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 ciascun 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 amministrative della soluzione, ovvero l'avvio manuale delle riparazioni o l'abilitazione della riparazione completamente automatizzata con regole. EventBridge Questo account deve inoltre essere l'account amministratore delegato di

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

Abilita AWS Config

Consulta la seguente documentazione:

- AWSDocumentazione Config
- AWSPrezzi Config
- Abilitazione di AWS Config

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

> **Important**
>
> Assicurati di selezionare l'opzione «Includi risorse globali (ad esempio, AWS IAM risorse)». Se non si seleziona questa opzione quando si attiva AWS Config, non verranno visualizzati i risultati relativi alle risorse globali (ad esempio AWS IAM le risorse)

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

Abilita l'hub AWS di sicurezza

Consulta la seguente documentazione:

- AWSDocumentazione Security Hub
- AWSPrezzi di Security Hub
- Abilitazione del AWS Security Hub

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

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 del controllo

Ai fini di questo tutorial, dimostreremo l'utilizzo della soluzione con la funzionalità di controllo consolidato 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, sarà necessario implementare i playbook specifici per gli standard anziché SC (Security Control).

Abilita 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 potrai 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:

- Aggregazione tra regioni
- Abilitazione dell'aggregazione tra regioni

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	Configurare l'aggregazione da us-west-2	Nessuno
222222222222	Membro	Configurare l'aggregazione da us-west-2	Nessuno

La propagazione dei risultati nella regione di aggregazione potrebbe richiedere del tempo. 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 del 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 seguente, utilizzeremo il metodo di invito manuale. Per un set di account di produzione, consigliamo di gestire l'amministrazione delegata di Security Hub tramite Organizations. AWS

Dalla console AWS Security Hub nell'account amministratore (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

Account	Scopo	Azione in us-east-1	Azione in us-west-2
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 li useremo. 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.

Implementa 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 Implementa lo stack di ruoli di esecuzione StackSet	Nessuno
222222222222	Membro	Implementa lo stack di ruoli di esecuzione StackSet	Nessuno

Crea le risorse non sicure che genereranno risultati di esempio

Consulta la seguente documentazione:

- Riferimento ai controlli del Security Hub
- AWSControlli Lambda

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

> **Important**
>
> Creeremo intenzionalmente una risorsa con una configurazione non sicura. Esamina la natura del controllo e valuta personalmente il rischio di creare una risorsa di questo tipo nel tuo ambiente. Siate consapevoli degli strumenti a disposizione della vostra organizzazione per rilevare e segnalare tali risorse e richiedete un'eccezione, se del caso. Se il controllo di esempio che abbiamo selezionato non è appropriato per te, 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 senza autenticazione. URL

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
222222222222	Membro	Nessuno	Creare una funzione Lambda con una configurazione non sicura

AWSConfig potrebbe impiegare del tempo per rilevare la configurazione non sicura. Puoi procedere con il tutorial, ma non sarai in grado di correggere il risultato finché Config non lo rileverà.

Crea gruppi di CloudWatch log per i controlli correlati

Consulta la seguente documentazione:

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

Vari CloudTrail controlli supportati dalla soluzione richiedono che sia presente un gruppo di CloudWatch log che sia la destinazione di una multiregione CloudTrail. Nell'esempio seguente, 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

Implementa la soluzione negli account tutorial

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

Implementa lo stack di amministrazione

View template

aws-sharr-deploy.modello

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 caricare gli stack di amministrazione annidati ad eccezione dello stack «SC» o «Security Control». Questo stack contiene le risorse per i risultati del controllo consolidato che abbiamo configurato nei nostri account.

Scegliete No di riutilizzare il gruppo di log di Orchestrator a meno che non abbiate già implementato questa soluzione in questo account e nella 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

Attendi che lo stack di amministrazione completi la distribuzione prima di continuare in modo da poter creare una relazione di fiducia tra gli account membro e l'account amministratore.

Distribuisci lo stack dei membri

View template

aws-sharr-member.modello

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

Immettete il nome del gruppo di log che avete creato come valore per il parametro per il nome del gruppo di log.

Scegli No il valore di tutti i parametri per caricare gli stack di membri annidati ad eccezione dello stack «SC» o «security control». Questo stack contiene le risorse per i risultati del controllo consolidato 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 è111111111111.

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

Implementa lo stack di ruoli dei membri

View template

aws-sharr-member-roles.modello

Nell'account amministratore, accedi alla CloudFormation StackSets console e distribuisci lo stack di membri su ciascun account. Usa i ruoli di StackSets amministratore 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 StackSet membro/Conferma lo stack di membri distribuito	Nessuno
222222222222	Membro	Conferma lo stack di membri distribuito	Nessuno

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

Iscriviti all'argomento SNS

Aggiornamenti di bonifica

Argomento - SO0111 - _Argomento SHARR

Nell'account amministratore, iscriviti all'SNSargomento Amazon creato dallo stack di amministrazione. Questo ti avviserà quando verranno avviate le riparazioni e se avranno esito positivo o negativo.

Allarmi

Argomento - SO0111 - _Alarm_Topic ASR

Nell'account amministratore, iscriviti all'SNSargomento Amazon creato dallo stack di amministrazione. Questo ti avviserà quando inizieranno gli allarmi metrici.

Correggi i risultati degli esempi

Nell'account amministratore, accedi alla console 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 dei controlli consolidati, una pagina denominata «Controlli» consente di individuare il risultato 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» ed eseguire la ricerca per attributo.

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

Avviare la riparazione

Seleziona la casella di controllo a sinistra del risultato relativo alla risorsa che abbiamo creato. Nel menu a discesa «Azioni», seleziona «Ripara con». ASR Verrà visualizzata una notifica che indica 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 SNS notifiche. 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 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

Traccia l'esecuzione della riparazione

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

EventBridge regola

Nell'account amministratore, individua una EventBridge regola denominata SHARRRemediate_with_ _. CustomAction Questa regola corrisponde al risultato inviato da Security Hub e lo invia a Orchestrator Step Functions.

Esecuzione di Step Functions

Nell'account amministratore, individua AWS Step Functions denominato "SO0111- SHARR - Orchestrator». Questa funzione di fase richiama il documento di SSM automazione nell'account e nella regione di destinazione. È possibile tracciare l'esecuzione della riparazione nella cronologia delle esecuzioni di questo AWS Step Functions.

Servizio di automazione di SSM

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

CloudWatch Gruppo di log

Nell'account amministratore, accedi alla console CloudWatch Logs e individua un gruppo di log denominato "SO0111 -». SHARR Questo gruppo di log è la destinazione dei log di alto livello di Orchestrator Step Functions.

Abilita riparazioni completamente automatizzate

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

Conferma di non disporre di risorse a cui questo risultato potrebbe essere applicato accidentalmente

L'attivazione delle riparazioni automatiche avvierà le riparazioni 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 riparazioni completamente automatizzate non saranno limitate alla funzione che avete creato. La soluzione correggerà questo controllo se viene rilevato in uno qualsiasi degli account e delle regioni in cui è installato.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Conferma nessuna funzione pubblica desiderata	Conferma nessuna funzione pubblica desiderata
222222222222	Membro	Conferma nessuna funzione pubblica desiderata	Conferma nessuna funzione pubblica desiderata

Abilita la regola

Nell'account Admin, individua una EventBridge regola denominata AutoTriggerSC_2.0.0_Lambda.1_ e abilitala.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Abilita le regole di riparazione automatizzate	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	Configurare la funzione Lambda per consentire l'accesso pubblico

Conferma che la correzione ha risolto il problema

Config potrebbe impiegare del tempo per rilevare nuovamente la configurazione non sicura. Dovresti ricevere due SNS notifiche. La prima indicherà che è stata avviata una riparazione. Il secondo indicherà che la riparazione è riuscita. Dopo aver ricevuto la seconda notifica, accedi alla console Lambda nell'account membro e conferma che l'accesso pubblico è stato revocato.

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

Eliminazione

Eliminate 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	Eliminare la funzione Lambda di esempio

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
222222222222	Membro	Nessuno	Nessuno

Elimina lo stack di membri

Nell'account amministratore, elimina il membro StackSet.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Eliminare 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 Amministratore, elimina i ruoli StackSet dei membri.

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

Account	Scopo	Azione in us-east-1	Azione in us-west-2
222222222222	Membro	Conferma l'elimina zione dello stack di ruoli dei membri	Nessuno

Elimina i ruoli mantenuti

In ogni account, elimina i ruoli mantenutiIAM.

Importante: questi ruoli vengono mantenuti per le riparazioni che richiedono un ruolo per continuare a funzionare (ad esempio VPC la registrazione del flusso). Conferma di non aver bisogno del 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	Eliminare i ruoli mantenuti	Nessuno
222222222222	Membro	Eliminare i ruoli mantenuti	Nessuno

Pianifica l'eliminazione delle KMS chiavi conservate

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

Queste chiavi vengono conservate per consentire l'accesso a tutte le risorse crittografate dalla soluzione. Conferma di non averle necessarie prima di programmarne l'eliminazione.

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

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Identifica e pianifica l'eliminazione della chiave di amministrazione Identifica e pianifica l'eliminazione della chiave membro	Identifica e pianifica l'eliminazione della chiave membro
222222222222	Membro	Identifica e pianifica l'eliminazione della chiave membro	Identifica e pianifica l'eliminazione della chiave membro

Elimina gli stack per le autorizzazioni StackSets autogestite

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 di ruoli di StackSet amministratore	Nessuno
222222222222	Membro	Eliminare lo stack di ruoli di StackSet esecuzione	Nessuno

Guida per sviluppatori

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

Codice sorgente

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

Playbook

Questa soluzione include i playbook correttivi per gli standard di sicurezza definiti nell'ambito di Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0, Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v3.0.0, CIS AWS AWS Foundational Security Best Practices (FSBP) v.1.0.0, Payment Card Industry Data Security Standard (-) v3.2.1 e National Institute of Standards PCI DSS https://docs.aws.amazon.com/securityhub/latest/userguide/nist-standard.htmle tecnologia (). NIST

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 Systems Manager con il nome distribuito dalla soluzione nel tuo account. Vai alla console AWS Systems Manager, quindi nel pannello di navigazione scegli Documenti.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
Rimediazioni 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 dello stato del sistema di bilanciamento del carico	Scalabilità automatica.1		Scalabilità automatica.1		Scalabilità automatica.1		Scalabilità automatica.1

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-CreateMultiRegionTrail CloudTrail deve essere attivato e configurato con almeno un percorso multiregionale	CloudTrail1.	2.1	CloudTrail2.	3.1	CloudTrail1.	3.1	CloudTrail1.
ASR-EnableEncryption CloudTrail dovrebbe avere la crittografia a riposo attivata	CloudTrail2.	2.7	CloudTrail1.	3.7	CloudTrail2.	3.5	CloudTrail2.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnableLogFileValidation Assicurarsi che la convalida dei file di CloudTrail registro sia attivata	CloudTrail4.	2.2	CloudTrail3.	3.2	CloudTrail4.		CloudTrail4.
ASR-EnableCloudTrailToCloudWatchLogging Assicurati che i CloudTrail percorsi siano integrati con Amazon CloudWatch Logs	CloudTrail5.	2.4	CloudTrail4.	3.4	CloudTrail5.		CloudTrail5.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-Configura S3 BucketLogging Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail		2.6		3.6		3.4	CloudTrail7.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-ReplaceCodeBuildClearTextCredentials CodeBuild le variabili di ambiente del progetto non devono contenere credenziali di testo non crittografato	CodeBuild 2.		CodeBuild 2.		CodeBuild 2.		CodeBuild 2.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnableAWSConfig Assicurarsi che AWS Config sia attivato	Config.1	2.5	Config.1	3.5	Config.1	3.3	Config.1
ASR-MakeEBSSnapshotsPrivato EBSLe istantanee di Amazon non devono essere ripristinabili pubblicamente	EC21.		EC21.		EC21.		EC21.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-RemoveVPCefaultSecurityGroupRules VPCIl gruppo di sicurezza predefinito dovrebbe vietare il traffico in entrata e in uscita	EC22.	4.3	EC22.	5.3	EC22.	5.4	EC22.
ASR-EregistrinableVPCFlow VPCla registrazione del flusso dovrebbe essere abilitata in tutti VPCs	EC26.	2.9	EC26.	3.9	EC2.6.	3.7	EC2.6.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnableEbsEncryptionByDefault EBSLa crittografia predefinita deve essere attivata	EC27.	2.2.1			EC27.	2.2.1	EC27.
ASR-RevokeUnrotatedKeys Le chiavi di accesso degli utenti devono essere ruotate ogni 90 giorni o meno	IAM3.	1.4		1.14	IAM3.	1.14	IAM3.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASRPolitica -SetIAMPassword IAMpolitica predefinita in materia di password	IAM7.	1,5-1,11	IAM8.	1.8	IAM7.	1.8	IAM7.
ASR-RevokeUnusedIAMUserCredentials Le credenziali utente devono essere disattivate se non utilizzate entro 90 giorni	IAM8.	1.3	IAM7.		IAM8.		IAM8.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-RevokeUnusedIAMUserCredentials Le credenziali utente devono essere disattivate se non utilizzate entro 45 giorni				1.12		1.12	IAM2.2
ASR-RemoveLambdaPublicAccess Le funzioni Lambda dovrebbero vietare l'accesso pubblico	Lambda.1		Lambda.1		Lambda.1		Lambda.1

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-MPrivatakeRDSSnpshot RDSLe istantane e dovrebber o vietare l'accesso pubblico	RDS1.		RDS1.		RDS1.		RDS1.
ASR-DisablePublicAccessToRDSInstance RDSLe istanze DB devono vietare l'accesso pubblico	RDS2.		RDS2.		RDS2.	2.3.3	RDS2.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EncryptRDSSnapshot RDSLe istantanee del cluster e le istantanee del database devono essere crittografate quando sono inattive	RDS4.				RDS4.		RDS4.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnableMultiAZOnRDSInstance RDSLe istanze DB devono essere configurate con più zone di disponibilità	RDS5.				RDS5.		RDS5.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnableEnhancedMonitoringOnRDSInstance Il monitoraggio avanzato deve essere configurato per le istanze e i cluster RDS DB	RDS6.				RDS.6.		RDS.6.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnableRDSCluster DeletionProtection RDSi cluster dovrebbero avere la protezione e dall'eliminazione attivata	RDS7.				RDS7.		RDS7.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnableRDSInstanceDeletionProtection RDSLe istanze DB devono avere la protezione da eliminazione attivata	RDS8.				RDS8.		RDS8.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnableMinorVersionUpgradeOnRDSDInstance RDSgli aggiornamenti automatici delle versioni minori devono essere attivati	RDS1.3				RDS.13	2.3.2	RDS.13

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnableCopyTagsToSnapshotOnRDSCluster RDSI cluster DB devono essere configurati per copiare i tag nelle istantanee	RDS1.6				RDS.16		RDS.16

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-DisablePublicAccessToRedshiftCluster I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico	Redshift.1		Redshift.1		Redshift.1		Redshift.1
ASR-EnableAutomaticSnapshotsOnRedshiftCluster I cluster Amazon Redshift devono avere snapshot automatici attivati	Redshift.3				Redshift.3		Redshift.3

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnableRedshiftClusterAuditLogging I cluster Amazon Redshift devono avere la registrazione di controllo attivata	Redshift.4				Redshift.4		Redshift.4

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnableAutomaticVersionUpgradeOnRedshiftCluster Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali attivati	Redshift.6				Redshift.6		Redshift.6

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-ConfiguraS3PublicAccessBlock L'impostazione 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-ConfiguraS3BucketPublicAccessBlock I bucket S3 dovrebbero vietare l'accesso pubblico in lettura	S3.2		S3.2	2.1.5.2	S3.2		S3.2

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-ConfigureS3BucketPublicAccessBlock I bucket S3 dovrebbero vietare l'accesso pubblico in scrittura		S3.3					S3.3
ASREnableDefaultEncryption-S3 I bucket S3 devono avere la crittografia lato server attivata	S3.4		S3.4	2.1.1	S3.4		S3.4

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASRetSSLBucketPolitica -S I bucket S3 dovrebbero richiedere e richieste per l'uso SSL	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5
ASR-S3 BlockDenylist Le autorizzazioni di Amazon S3 concesse ad altre policy Account AWS in bucket devono essere limitate	S3.6				S3.6		S3.6

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
L'impostazione S3 Block Public Access deve essere attivata a livello di bucket	S3.8				S3.8		S3.8
ASR-Configura S3 BucketPublicAccessBlock Assicurati che i log del bucket CloudTrail S3 non siano accessibili al pubblico		2.3					CloudTrail6.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-CreateAccessLoggingBucket Assicurati che la registrazione degli accessi al bucket S3 sia attivata sul bucket S3 CloudTrail		2.6					CloudTrail7.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnableKeyRotation Assicurati che la rotazione creata dal cliente CMKs sia attivata		2.8	KMS1.	3.8	KMS4.	3.6	KMS4.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Assicurati che esistano un registro, un filtro metrico e un allarme per le chiamate non API autorizzate		3.1		4.1			Cloudwatch.1

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Assicurati che esistano un filtro metrico di registro e un allarme per l'accesso senza AWS Management Console MFA		3.2		4.2			Cloudwatch.2

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Assicurati che esistano un filtro metrico di registro e un allarme per l'utilizzo dell'utente «root»		3.3	CW.1	4.3			Cloudwatch 3

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle politiche IAM		3.4		4.4			Cloudwatch 4

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alla configurazione CloudTrail		3.5		4.5			Cloudwatch 5

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Assicurati che esistano un filtro metrico di registro e un allarme per gli errori di autenticazione AWS Management Console		3.6		4.6			Cloudwatch 6

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione programmata dei dati creati dal cliente CMKs		3.7		4.7			Cloudwatch 7

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle policy dei bucket S3		3.8		4.8			Cloudwatch 8

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alla configurazione AWS Config		3.9		4.9			Cloudwatch.9

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate al gruppo di sicurezza		3.10		4,10			Cloudwatch.10

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche agli elenchi di controllo degli accessi alla rete () NACL		3.11		4,11			Cloudwatch.11

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate ai gateway di rete		3.12		4,12			Cloudwatch.12

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle tabelle di routing		3.13		4.13			Cloudwatch.13

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche VPC		3.14		4,14			Cloudwatch 14

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
AWS-DisablePublicAccessForSecurityGroup Assicurati che nessun gruppo di sicurezza consenta l'ingresso dalla porta 0.0.0.0/0 alla porta 22		4.1	EC25.		EC21.3		EC2.13

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
AWS-DisablePublicAccessForSecurityGroup Assicurati che nessun gruppo di sicurezza consenta l'ingresso dalla porta 0.0.0.0/0 alla porta 3389		4.2			EC21.4		EC2.14
ASR-ConfigureSNSTopicForStack	CloudFormation1.				CloudFormation1.		CloudFormation1.
ASR-CreateIAMSupportRuolo		1.20		1,17		1,17	IAM.18

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-DisablePublicIPAutoAssign Le EC2 sottoreti Amazon non devono assegnare automaticamente indirizzi IP pubblici	EC21.5				EC2.15		EC2.15
ASR-EnableCloudTrailLogFileValidation	CloudTrail4.	2.2	CloudTrail3.	3.2			CloudTrail4.
ASR-EnableEncryptionForSNSTopic	SNS1.				SNS1.		SNS1.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnableDeliveryStatusLoggingForSNSTopic La registrazione dello stato di consegna deve essere abilitata per i messaggi di notifica inviati a un argomento	SNS2.				SNS2.		SNS2.
ASR-EnableEncryptionForSQSQueue	SQS1.				SQS1.		SQS1.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-MPrivatakeRDSSnpshot RDSl'istantanea deve essere privata	RDS1.		RDS1.				RDS1.
ASR-BlockSSMDocumentPublicAccess SSMI documenti non devono essere pubblici	SSM4.				SSM4.		SSM4.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnableCloudFrontDefaultRootObject CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato	CloudFront1.				CloudFront1.		CloudFront1.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-SetCloudFrontOriginDomain CloudFront le distribuzioni non devono puntare a origini S3 inesistenti	CloudFront.2				CloudFront.12		CloudFront.12

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-RemoveCodeBuildPrivilegedMode CodeBuild gli ambienti di progetto devono avere una durata di registrazione AWS Config	CodeBuild 5.				CodeBuild 5.		CodeBuild 5.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-TerminaEC2Instance EC2Le istanze interrotte devono essere rimosse dopo un periodo di tempo specificato	EC24.				EC24.		EC24.
ASR-AbilitaIMDSV2Onnstance EC2le istanze devono utilizzare Instance Metadata Service versione 2 () IMDSv2	EC28.				EC28.	5.6	EC28.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-RevokeUnauthorizedInboundRules I gruppi di sicurezza dovrebbero consentire il traffico in entrata senza restrizioni solo per le porte autorizzate	EC21.8				EC2.18		EC2.18

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR- tDisableUnrestrictedAccessToHighRiskPorts I gruppi di sicurezza non dovrebbero consentire l'accesso illimitato alle porte ad alto rischio	EC21.9				EC2.19		EC2.19

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-DisableTGWAutoAcceptSharedAttachments Amazon EC2 Transit Gateways non dovrebbe accettare automaticamente le richieste di VPC allegati	EC22.3				EC2.23		EC2.23

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnablePrivateRepositoryScanning ECRi repository privati dovrebbero avere la scansione delle immagini configurata	ECR1.				ECR1.		ECR1.
ASR-EnableGuardDuty GuardDuty dovrebbe essere abilitato	GuardDuty 1.		GuardDuty 1.		GuardDuty 1.		GuardDuty 1.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-ConfiguraS3BucketLogging La registrazione degli accessi al server bucket S3 deve essere abilitata	S3.9				S3.9		S3.9
ASR-EnableBucketEventNotifications I bucket S3 devono avere le notifiche degli eventi abilitate	S3.11				S3.11		S3.11

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-Imposta S3 Lifecycle Policy I bucket S3 devono avere politiche del ciclo di vita configurate	S3.13				S3.13		S3.13
ASR-EnableAutoSecretRotation I segreti di Secrets Manager devono avere la rotazione automatica abilitata	SecretsManager1.				SecretsManager1.		SecretsManager1.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-RemoveUnusedSecret Rimuovi i segreti inutilizzati di Secrets Manager	SecretsManager3.				SecretsManager3.		SecretsManager3.
ASR-UpdateSecretRotationPeriod I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni	SecretsManager4.				SecretsManager4.		SecretsManager4.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnableAPIGatewayCacheDataEncryption APII dati REST API della cache del gateway devono essere crittografati quando sono inattivi					APIGateway5.		APIGateway5.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-SetLogGroupRetentionDays CloudWatch i gruppi di log devono essere conservati per un periodo di tempo specificato					CloudWatch1.6		CloudWatch.16

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-AttachServiceVPCEndpoint Amazon EC2 deve essere configurato per utilizzare VPC gli endpoint creati per il servizio AmazonEC.	EC2.10				EC2.10		EC2.10
ASR-TagGuardDutyResource GuardDuty i filtri devono essere etichettati							GuardDuty 2.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-TagGuardDutyResource GuardDuty i rilevatori devono essere etichettati							GuardDuty 4.
ASR-AttachSSMPermissions EC2 EC2Le istanze Amazon devono essere gestite da Systems Manager	SSM1.		SSM3.				SSM1.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-ConfigureLaunchConfigNoPublicIPDocument EC2Le istanze Amazon lanciate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici.					Autoscaling.5		Autoscaling.5
ASR-EnableAPIGatewayExecutionLogs	APIGateway1.						APIGateway1.

Descrizione	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	ID di controllo di sicurezza
ASR-EnableMacie Amazon Macie dovrebbe essere abilitato	Macie.1				Macie.1		Macie.1
ASR-EnableAthenaWorkGroupLogging I gruppi di lavoro Athena devono avere la registrazione abilitata	Atena.4						Atena.4

Aggiungere nuove correzioni

L'aggiunta di una nuova correzione a un playbook esistente non richiede modifiche alla soluzione stessa.

> **Note**
>
> Le istruzioni che seguono sfruttano le risorse installate dalla soluzione come punto di partenza. Per convenzione, la maggior parte dei nomi di risorse delle soluzioni contiene SHARRe/o SO0111 per facilitarne l'individuazione e l'identificazione.

Panoramica

Automated Security Response sui AWS runbook deve seguire la seguente denominazione standard:

`ASR-<standard>-<version>-<control>`

Standard: l'abbreviazione dello standard di sicurezza. Questo deve corrispondere agli standard supportati daSHARR. 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 SHARR e alla versione contenuta nei dati di ricerca.

Controllo: l'ID del controllo da correggere. Deve corrispondere ai dati di ricerca.

1. Crea un runbook negli account dei membri.
2. Crea un IAM ruolo negli account dei membri.
3. (Facoltativo) Crea una regola di correzione automatica nell'account amministratore.

Fase 1: Crea un runbook negli account dei membri

1. Accedi alla AWS Systems Manager console e ottieni un esempio del risultatoJSON.
2. Crea un runbook di automazione che corregga il risultato. Nella scheda Owned by me, usa uno qualsiasi dei `ASR-` documenti nella scheda Documenti come punto di partenza.
3. L' AWS Step Functions account dell'amministratore eseguirà il tuo runbook. Il runbook deve specificare il ruolo di correzione da passare quando si chiama il runbook.

Fase 2: Crea un IAM ruolo negli account dei membri

1. Accedi alla console AWS Identity and Access Management.

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 il controllo CIS v1.2.0 5.6, il ruolo deve essere. `SO0111-Remediate-CIS-1.2.0-5.6`
3. Utilizzando l'esempio, create un ruolo con un ambito appropriato che consenta solo le API chiamate necessarie per eseguire la correzione.

A questo punto, la riparazione è attiva e disponibile per la riparazione automatica dall'Azione SHARR personalizzata in AWS Security Hub.

Passaggio 3: (Facoltativo) Crea una regola di riparazione automatica nell'account amministratore

La riparazione automatica (non «automatizzata») è l'esecuzione immediata della riparazione non appena il risultato viene ricevuto da AWS Security Hub. Valuta attentamente i rischi prima di utilizzare questa opzione.

1. Visualizza una regola di esempio per lo stesso standard di sicurezza in CloudWatch Events. Lo standard di denominazione per le regole è`standard_control_`**`AutoTrigger`**.
2. Copia il modello di evento dall'esempio da utilizzare.
3. Modifica il `GeneratorId` valore in modo che corrisponda a quello `GeneratorId` indicato nel tuo FindingJSON.
4. Salva e attiva la regola.

Aggiungere un nuovo playbook

Scaricate l'Automated Security Response on AWS Solution Playbook e il codice sorgente di distribuzione dal GitHub repository.

Le AWS CloudFormation risorse vengono create a partire dai AWS CDKcomponenti 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.md in. README GitHub

AWS Systems Manager Archivio dei parametri

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	Utilizza
`/Solutions/SO0111/CMK_REMEDIATION_ARN`	AWS KMS chiave che crittograferà i dati per le FSBP riparazioni	Crittografia dei dati dei clienti, come CloudTrail i registri, come parte delle correzioni
`/Solutions/SO0111/CMK_ARN`	AWS KMS chiave che SHARR verrà utilizzata per crittografare i dati	Crittografia dei dati della soluzione
`/Solutions/SO0111/SNS_Topic_ARN`	ARNdell'SNSargomento Amazon per la soluzione	Notifica degli eventi di riparazione
`/Solutions/SO0111/SNS_Topic_Config.1`	SNSargomento per gli aggiornamenti AWS Config	Correzione Config.1
`/Solutions/SO0111/sendAnonymousMetrics`	`Yes`	Raccolta di metriche anonimizzate
`/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 riparazione automatica modificandolo in `disabled`
`/Solutions/SO0111/ <security standard long name>/shortname`	`String`	Nome abbreviato dello standard di sicurezza. Ad esempio: 'CIS', 'AFSBP', 'PCI'

Nome	Valore	Utilizza
/Solutions/SO0111/ *<security standard long name>*/*<version>* /*<control>* /remap	String	Quando un controllo utilizza la stessa correzione di un altro, questi parametri eseguono la rimappatura

SNSArgomento Amazon - Progresso della riparazione

Automated Security Response on AWS crea un SNS argomento Amazon, SO0111- SHARR _Topic. Questo argomento viene utilizzato per pubblicare aggiornamenti sullo stato di avanzamento della riparazione. Di seguito sono riportate le tre possibili notifiche inviate a questo argomento.

```
Remediation queued for <standard> control <control_ID> in account <account_ID>
```

```
Remediation failed for <standard> control <control_ID> in account <account_ID>
```

```
<control_ID> remediation was successfully invoke via AWS Systems Manager in
 account <account_ID>
```

Questo è il messaggio di completamento. Indica che la riparazione è stata completata senza errori; tuttavia, il test definitivo per una corretta correzione è il controllo di Config e/o la AWS convalida manuale.

Filtrare l'abbonamento a un argomento SNS

Politiche di filtro degli SNS abbonamenti Amazon:

1. Vai alla sottoscrizione dell'SNSargomento.
2. In Politica di filtro degli abbonamenti, seleziona «Modifica».
3. Espandi «Politica di filtro degli abbonamenti» e attiva l'opzione «Politica di filtro degli abbonamenti» per abilitare i filtri.
4. Seleziona l'ambito «Corpo del messaggio».
5. Aggiungi la tua politica all'JSONeditor.
6. Salva le modifiche.

Politiche di esempio:

Filtra per account

```
{
    "finding": {
      "account": [
        "111111111111",
        "222222222222"
      ]
    }
```

Filtra per errori

```
{
    "severity": ["ERROR"]
    }
```

Filtra per controlli

```
{
    "finding": {
       "standard_control": ["S3.9","S3.6"]
      }
   }
```

SNSArgomento Amazon: CloudWatch allarmi

Questa soluzione crea un SNS argomento Amazon,`SO0111-ASR_Alarm_Topic`. Questo argomento viene utilizzato per pubblicare avvisi di allarme.

I dettagli di tutti gli allarmi che entrano nello ALARM stato verranno inviati a questo argomento.

Avvia Runbook su Config Findings

Questa soluzione può avviare runbook basati su risultati personalizzati. AWS Config A tale scopo è necessario:

1. Trova il nome della AWS Config regola a cui desideri correggere. Questo può essere trovato in uno AWS Config o nei risultati generati da Security Hub per questa regola.
2. Accedere a AWS Systems Manager Parameter Store e selezionare Crea parametro.
3. Il nome della regola deve essere `/Solutions/SO0111/`*`Rule name from Step 1`*
4. Il valore deve essere formattato come segue:

```
{

"RunbookName":"Name of SSM runbook",

"RunbookRole": "Role that Orchestrator will assume"

}
```

5. RunbookName è un campo obbligatorio e sarà il runbook che viene eseguito quando si corregge questa regola di Config. RunbookRole è il ruolo che l'orchestratore assumerà durante l'esecuzione di questo ruolo. Non è un campo obbligatorio e, se omesso, l'orchestratore utilizzerà per impostazione predefinita il ruolo di membro dell'account.
6. Una volta completata questa operazione, puoi correggere la regola di Config utilizzando l'azione personalizzata «Ripara ASR con» disponibile nel Security Hub.

Riferimento

Questa sezione include informazioni su una funzionalità opzionale per la raccolta di metriche uniche per questa soluzione, riferimenti a risorse correlate e un elenco di costruttori che hanno contribuito a questa soluzione.

Raccolta di dati anonimizzata

Questa soluzione include un'opzione per inviare metriche operative anonime a. AWS Utilizziamo questi dati per comprendere meglio come i clienti utilizzano questa soluzione e i servizi e i prodotti correlati. Se abilitata, le seguenti informazioni vengono raccolte e inviate a: AWS

- ID della soluzione: l'identificatore della AWS soluzione
- ID univoco (UUID): identificatore univoco generato casualmente per ogni AWS Security Hub implementazione di Response and Remediation
- Timestamp: timestamp di raccolta dati
- Dati dell'istanza: informazioni sulla distribuzione di questo stack
- CloudWatchMetricsDashboardEnabled- `"Yes"` se CloudWatch Metrics e Dashboard sono abilitati durante la distribuzione
- Stato: stato della distribuzione (soluzione approvata o non riuscita) o (riparazione approvata o fallita)
- Messaggio di errore: il messaggio di errore generico nel campo dello stato
- Generator_ID - Informazioni sulle regole del Security Hub
- Tipo: tipo e nome della riparazione
- productArn- La regione in cui viene distribuito Security Hub
- finding_triggered _ by - Il tipo di riparazione eseguita (azione personalizzata o attivazione automatica)

AWSpossiede i dati raccolti attraverso questo sondaggio. La raccolta dei dati è soggetta all'AWSInformativa sulla privacy. Per disattivare questa funzionalità, completa i seguenti passaggi prima di avviare il AWS CloudFormation modello.

1. Scarica il AWS CloudFormation modello sul tuo disco rigido locale.

2. Apri il AWS CloudFormation modello con un editor di testo.
3. Modifica la sezione AWS CloudFormation di mappatura dei modelli da:

```
Mappings:
  Solution:
    Data:
      SendAnonymizedUsageData: 'Yes'
```

to:

```
  Mappings:
    Solution:
      Data:
        SendAnonymizedUsageData: 'No'
```

4. Accedere alla console AWS CloudFormation .
5. Seleziona Crea pila.
6. Nella pagina Crea stack, sezione Specificare il modello, seleziona Carica un file modello.
7. In Carica un file modello, scegli Scegli file e seleziona il modello modificato dall'unità locale.
8. Scegli Avanti e segui i passaggi descritti in Avvia lo stack nella sezione Distribuzione automatizzata di questa guida.

Risorse correlate

- Risposta e correzione automatizzate con AWS Security Hub
- CISBenchmark di Amazon Web Services Foundations, versione 1.2.0
- AWS Foundational Security Best Practices standard
- Standard di sicurezza dei dati del settore delle carte di pagamento () 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 Schuetter
- Andrew Yankowsky
- Josh Moss
- Ryan Garay
- Thiemo Belmega

Revisioni

Data	Modifica
agosto 2020	Rilascio iniziale
ottobre 2020	Sono state aggiunte ulteriori informazioni sulla risoluzione dei problemi all'Appendice C.
Novembre 2020	Sono state aggiunte istruzioni di distribuzione per le regioni della Cina; istruzioni di distribuz ione della soluzione aggiornate per l'account amministratore di Security Hub; per ulteriori informazioni, fare riferimento al CHANGELOG file.md nel GitHub repository.
aprile 2021	Versione v1.2.0: aggiunta una nuova architett ura del playbook e nuove correzioni. FSBP Per ulteriori informazioni, consulta il CHANGELOG file.md nel repository. GitHub
maggio 2021	Versione v1.2.1: correzione di un problema che riguardava EC2 .2 e .7. EC2 Per ulteriori informazioni, consulta il CHANGELOGfile.md nel repository. GitHub
agosto 2021	Versione v1.3.0: aggiunto il playbook PCI DSS v3.2.1. Aggiunte 17 nuove correzioni alla v1.2.0. CIS Sono state aggiunte quattro nuove correzioni a. FSBP Convertito CIS per utilizzar e una nuova architettura di playbook basata sui SSM runbook. Sono state aggiunte istruzioni per estendere i playbook esistenti con correzion i definite dal cliente. Per ulteriori informazioni, consulta il CHANGELOGfile.md nel repository. GitHub

Data	Modifica
settembre 2021	Versione v1.3.1: `CreateLogMetricFilterAndAlarm.py` modificata per rendere attive le azioni, aggiungi SNS una notifica a. `SO0111-SHARR-LocalAlarmNotification` Modificata la correzione CIS 2.8 per adattarla al nuovo formato dei dati di ricerca. Per ulteriori informazioni, fate riferimento al CHANGELOGfile.md nel repository. GitHub
novembre 2021	Versione v1.3.2: correzioni di bug per i controlli CIS v1.2.0 3.1 - 3.14. Per ulteriori informazioni, consulta il file.md nel CHANGELOG repository. GitHub
Dicembre 2021	Versione v1.4.0: la soluzione può ora essere distribuita utilizzando. StackSets La riparazione tra regioni è ora supportata oltre alla correzione tra account. IAMI ruoli degli account membro vengono ora mantenuti quando lo stack viene rimosso. Per ulteriori informazioni, consulta il CHANGELOGfile.md nel repository. GitHub
Gennaio 2022	Versione v1.4.1: correzioni di bug. Per ulteriori informazioni, consulta il CHANGELOGfile.md nel repository. GitHub
Gennaio 2022	Versione v1.4.2: correzioni di bug. Per ulteriori informazioni, consulta il CHANGELOGfile.md nel repository. GitHub
giugno 2022	Versione v1.5.0: correzioni aggiuntive. Per ulteriori informazioni, fare riferimento al CHANGELOGfile.md nel repository. GitHub

Data	Modifica
Dicembre 2022	Versione 1.5.1 Modifiche per passare la creazione di SSM documenti da Custom Resource `CfnDocument` Lambda a. Il prefisso per i nomi dei SSM documenti viene aggiornato per iniziare con ASR invece di. SHARR Per ulteriori informazioni, fate riferimento al CHANGELOGfile.md nel repository. GitHub
Marzo 2023	Versione 2.0.0: è stato aggiunto il supporto per i controlli di sicurezza e gli standard CIS v1.4.0, cinque nuove correzioni agli FSBP standard, una nuova correzione agli standard CIS v1.2.0, l' AppRegistry integrazione del catalogo dei servizi e protezioni aggiuntive per evitare errori di distribuzione dovuti alla limitazione dei documenti. SSM Per ulteriori informazioni, consulta il file.md nel repository. CHANGELOG GitHub
Aprile 2023	Versione 2.0.1: Impatto mitigato causato dalle nuove impostazioni predefinite per S3 Object Ownership (ACLsdisabilitate) per tutti i nuovi bucket S3. Per ulteriori informazioni, consulta il CHANGELOGfile.md nel repository. GitHub
Maggio 2023	Aggiornamento della documentazione: definizioni Well-Architected aggiornate, linee guida aggiuntive su dove distribuire ogni stack, edizione aggiuntiva di Troubleshooting dei problemi con soluzioni specifiche ed esempi di codice aggiornati nelle notifiche. SNS

Data	Modifica
Luglio 2023	Aggiornamento della documentazione: aggiornato il diagramma dell'architettura e i componenti della soluzione nel flusso di lavoro.
Ottobre 2023	Versione 2.0.2: versioni aggiornate dei pacchetti per risolvere le vulnerabilità di sicurezza. Per ulteriori informazioni, consulta il CHANGELOGfile.md nel repository. GitHub
Novembre 2023	Aggiornamento della documentazione: è stata aggiunta la conferma dei tag di costo associati alla soluzione nella AppRegistry sezione Monitoraggio della soluzione con AWS Service Catalog.
Marzo 2024	Versione 2.1.0: è stato aggiunto il supporto per NIST lo standard, sono state aggiunte 17 nuove correzioni FSBP agli standard, è stato aggiunto il CloudWatch dashboard per la soluzione di monitoraggio, è stato aggiunto il gestore di throttling all'architettura, è stato aggiunto il supporto per i parametri di input personalizzabili di Security Hub e aggiunto il supporto per la correzione dei risultati di Config. Per ulteriori informazioni, consulta il file.md nel repository. CHANGELOG GitHub
aprile 2024	Versione 2.1.1: Aggiornamento all'ordine CloudFormation dei parametri e ai valori predefiniti Aggiornamento della documenta zione. Aggiunti riferimenti allo NIST standard. Sono state aggiunte informazioni relative alle quote di servizio delle EventBridge regole. Per ulteriori informazioni, fare riferimento al CHANGELOGfile.md nel repository. GitHub

Data	Modifica
Giugno 2024	Versione 2.1.2: disabilitata AppRegistry per alcuni playbook per evitare errori durante l'aggiornamento della soluzione. Per ulteriori informazioni, consulta il CHANGELOGfile.md nel repository. GitHub
Settembre 2024	Versione 2.1.3: è stato risolto un problema negli script di riparazione per EC2 .18 e EC2 .19 a causa del quale le regole dei gruppi di sicurezza IpProtocol impostate su -1 venivano erroneamente ignorate. Sono stati aggiornati tutti i runtime Python nei documenti di riparazio ne da Python SSM 3.8 a Python 3.11. Per ulteriori informazioni, consulta il file.md nel repository. CHANGELOG GitHub
Novembre 2024	Versione 2.1.4: runtime Python aggiornati in tutti i runbook di controllo da Python 3.8 a Python 3.11. Per ulteriori informazioni, fate riferimento al file.md nel repository. CHANGELOG GitHub
dicembre 2024	Versione 2.2.0: aggiunta l'integrazione del sistema di biglietteria, CloudTrail Action Log e CIS il playbook 3.0.0. Dashboard e notifiche migliorate. Per ulteriori informazioni, consulta il CHANGELOGfile.md nel GitHub repository.

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 AWS attuali offerte e pratiche di prodotto, che sono soggette a modifiche senza preavviso, e (c) non crea alcun impegno o garanzia da parte AWS delle sue affiliate, fornitori o licenzianti. AWS i prodotti o i servizi sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite. AWS le responsabilità nei confronti dei propri clienti sono regolate da AWS accordi e il presente documento non fa parte di, né modifica, alcun accordo tra AWS e i suoi clienti.

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.