Guida per l'utente

Agente di sicurezza AWS

Agente di sicurezza AWS: Guida per l’utente

Table of Contents

Introduzione

Scopri cosa fa AWS Security Agent, come funziona e come le sue risorse si integrano tra loro.

Cos'è AWS Security Agent?

AWS Security Agent è un agente di frontiera che protegge in modo proattivo le tue applicazioni durante tutto il ciclo di vita dello sviluppo. Conduce revisioni di sicurezza automatizzate personalizzate in base ai requisiti organizzativi, crea modelli di minaccia per identificare in che modo le applicazioni potrebbero essere attaccate e fornisce test di penetrazione sensibili al contesto su richiesta. Convalidando continuamente la sicurezza dalla progettazione alla distribuzione, AWS Security Agent aiuta a prevenire tempestivamente le vulnerabilità in tutti gli ambienti.

I team di sicurezza definiscono i requisiti di sicurezza organizzativi una volta nella console AWS: librerie di autorizzazione approvate, standard di registrazione e politiche di accesso ai dati. AWS Security Agent applica automaticamente questi requisiti di sicurezza durante lo sviluppo, valutando i documenti e il codice dell'architettura rispetto agli standard e fornendo linee guida specifiche quando rileva violazioni. Ciò garantisce un'applicazione coerente della sicurezza per la progettazione e la revisione del codice in tutti i team.

Per la convalida dell'implementazione, AWS Security Agent trasforma i test di penetrazione da collo di bottiglia periodico a funzionalità on-demand. I team di sicurezza forniscono gli URL di destinazione, i dettagli di autenticazione, il codice sorgente e la documentazione dell'applicazione. AWS Security Agent sviluppa una comprensione approfondita delle applicazioni ed esegue sofisticate catene di attacco per scoprire e convalidare le vulnerabilità, consentendo ai team di eseguire test ogni volta che è necessario.

Funzionalità chiave

AWS Security Agent offre funzionalità di sicurezza complete che coprono l'intero ciclo di vita dello sviluppo.

Revisione della sicurezza del progetto

AWS Security Agent modifica la sicurezza fornendo feedback sulla sicurezza in tempo reale sui documenti di progettazione e valutando la conformità ai requisiti di sicurezza organizzativi prima della scrittura di qualsiasi codice. I team di sicurezza caricano i documenti tramite l'applicazione Web e ricevono indicazioni sulla correzione per dare priorità ai risultati, accelerando le lunghe revisioni

manuali trasformandole in analisi mirate. Integrando in modo proattivo gli standard di sicurezza in ogni revisione del progetto, è possibile ridurre le rielaborazioni architettoniche in fase avanzata e tenere il passo con i diversi team di sviluppo.

Modellazione delle minacce

AWS Security Agent crea modelli di minaccia delle tue applicazioni per identificare come potrebbero essere attaccate. Fornisci documenti tecnici di progettazione (documenti di ambito) per definire su cosa si concentra l'agente, codice sorgente come contesto in cui l'agente può comprendere il sistema esistente o entrambi. AWS Security Agent genera una panoramica del sistema che descrive l'architettura, i componenti, i limiti di fiducia, i flussi di dati e il livello di sicurezza dell'applicazione, insieme a una serie di minacce classificate per categoria STRIDE (spoofing, tampering, ripudiation, information disclosure, Denial of Service, Elevation of Privilege) con livelli di gravità e raccomandazioni attuabili. I modelli di minaccia sono configurazioni riutilizzabili che è possibile rieseguire man mano che il codice e la progettazione si evolvono, consentendo una valutazione iterativa della sicurezza durante l'intero ciclo di vita dello sviluppo.

Revisione della sicurezza del codice

AWS Security Agent protegge in modo proattivo le applicazioni attraverso due approcci complementari. Innanzitutto, puoi creare revisioni del codice nell'applicazione Web per eseguire scansioni complete del codice sorgente completo proveniente dai repository Bitbucket o GitHub Enterprise Server o dai GitHub bucket S3, identificando le vulnerabilità di sicurezza e convalidando la conformità ai requisiti organizzativi nell'intera base di codice. GitLab In secondo luogo, puoi abilitare l'analisi automatizzata delle pull request per i repository connessi, in cui AWS Security Agent esamina le modifiche al codice e pubblica i risultati di sicurezza direttamente come commenti di pull request o merge request. In entrambi i casi, gli sviluppatori ricevono indicazioni sulla correzione e AWS Security Agent può generare automaticamente richieste pull o unire richieste con correzioni di codice per le vulnerabilità identificate. Ciò integra le competenze in materia di sicurezza in tutti gli archivi, riducendo i ritardi legati alla sicurezza nella pipeline di sviluppo e scalando la valutazione su tutte le basi di codice.

Test di penetrazione (pen-test)

AWS Security Agent offre test di penetrazione su richiesta implementando agenti di intelligenza artificiale specializzati per scoprire, convalidare, segnalare e correggere le vulnerabilità di sicurezza attraverso scenari di attacco personalizzati in più fasi. L'agente comprende il contesto dell'applicazione analizzando il codice sorgente e la documentazione per identificare e sfruttare

le vulnerabilità che gli strumenti di scansione di sicurezza automatizzati non riescono a rilevare. Documenta i risultati con analisi dell'impatto, percorsi di attacco riproducibili e crea pull request con correzioni di codice pronte per l'implementazione, trasformando le valutazioni periodiche in una convalida continua che si adatta a tutte le applicazioni anziché limitarsi solo a quelle critiche.

Vantaggi

On-demand accessibilità

AWS Security Agent fornisce un accesso immediato alle competenze in materia di sicurezza. I team di sviluppo possono eseguire revisioni di progettazione, modelli di minaccia, analisi del codice e test di penetrazione su richiesta ogni volta che è necessario, adattandosi al ritmo dei cicli di sviluppo moderni e garantendo una sicurezza proattiva in ogni fase.

Convalida automaticamente i requisiti organizzativi

Definisci i requisiti di sicurezza della tua organizzazione una volta nella console AWS. AWS Security Agent convalida automaticamente questi requisiti in tutte le applicazioni durante ogni revisione della progettazione e della sicurezza del codice, garantendo che i team soddisfino i requisiti specifici anziché elenchi di controllo generici.

Esperienza di sicurezza scalabile

AWS Security Agent ridimensiona le revisioni di sicurezza per adeguarle alla velocità di sviluppo automatizzando l'applicazione dei requisiti di sicurezza organizzativi. Configura i requisiti a livello centrale, esegui revisioni complete con analisi dei risultati e gestisci gli ambiti dei test di penetrazione in tutta l'organizzazione tramite la console AWS.

Correzioni attuabili per vulnerabilità confermate

AWS Security Agent convalida i risultati di sicurezza rilevati durante i test di penetrazione attraverso uno sfruttamento basato su prove, fornendo percorsi di exploit riproducibili, analisi di impatto complete e crea pull request con correzioni pronte da implementare in un linguaggio adatto agli sviluppatori. Questo aiuta i team a concentrarsi sui rischi di sicurezza legittimi ad alto impatto senza perdere tempo con falsi positivi.

Supporto cloud multiplo e ibrido

AWS Security Agent opera in ambienti AWS, on-premise, ibridi, multicloud e SaaS, garantendo linee guida e test di sicurezza coerenti indipendentemente dalle scelte di infrastruttura o piattaforma.

Funzionalità di AWS Security Agent

AWS Security Agent offre quattro funzionalità di sicurezza di base per tutto il ciclo di vita dello sviluppo:

- Revisione della sicurezza del progetto: esamina i documenti di progettazione e architettura per identificare i rischi per la sicurezza. Carica i documenti tramite l'applicazione web e il servizio li analizza in base ai requisiti di sicurezza dell'organizzazione. AWS Security Agent valuta la conformità ai requisiti di sicurezza definiti, come le librerie di autorizzazione approvate, gli standard di registrazione e le politiche di accesso ai dati. In questo modo è possibile individuare progetti non sicuri e violazioni delle policy fin dalle prime fasi del processo di sviluppo.
- Modellazione delle minacce: crea un modello di minaccia dell'applicazione per identificare come potrebbe essere attaccata. Fornite i documenti di progettazione come documenti di riferimento per definire l'obiettivo dell'analisi, il codice sorgente come contesto per consentire all'agente di comprendere il sistema esistente o entrambi. AWS Security Agent genera una panoramica del sistema che descrive l'architettura, i componenti, i limiti di fiducia, i flussi di dati e il livello di sicurezza dell'applicazione, insieme a una serie di minacce classificate per categoria STRIDE (spoofing, tampering, ripudiation, information disclosure, Denial of Service, Elevation of Privilege) con livelli di gravità e raccomandazioni attuabili. Ogni minaccia si ricollega alle prove contenute nel codice sorgente.
- Revisione della sicurezza del codice: analizza il codice contenuto nei tuoi repository e nelle fonti S3 per identificare vulnerabilità di sicurezza e violazioni dei requisiti di sicurezza organizzativi in tutti i linguaggi, i framework e le architetture. Crea revisioni del codice nell'applicazione web per eseguire scansioni complete del codice sorgente completo o abilita i commenti pull request per rivedere automaticamente le modifiche al codice. GitHub AWS Security Agent fornisce linee guida specifiche per la correzione e può generare automaticamente richieste pull con correzioni di codice per le vulnerabilità identificate. Ciò garantisce l'applicazione coerente delle tue politiche di sicurezza in tutti i team di sviluppo.
- On-demand test di penetrazione: rileva, convalida, segnala e corregge le vulnerabilità di sicurezza nelle applicazioni Web e nelle API live attraverso scenari di attacco personalizzati in più fasi. Configura il servizio per creare un pentest tramite l'applicazione web specificando l'ambito del test, i dettagli di autenticazione e le risorse. AWS Security Agent sviluppa il contesto applicativo a partire dal codice sorgente e dalla documentazione forniti ed esegue sofisticate catene di attacco per identificare le vulnerabilità sfruttabili che l'analisi statica e gli strumenti convenzionali sfuggono. Fornisce inoltre correzioni di codice pronte per l'implementazione e crea richieste pull direttamente nel tuo repository di codice, consentendoti di risolvere le vulnerabilità ancora più velocemente.

Come funziona AWS Security Agent

AWS Security Agent opera su tre interfacce per fornire una sicurezza proattiva delle applicazioni durante tutto il ciclo di vita dello sviluppo. Le configurazioni di sicurezza vengono gestite nella Console di gestione AWS, le revisioni di sicurezza vengono condotte nell'applicazione Web Security Agent e la correzione automatica del codice e dei risultati di sicurezza avviene direttamente in piattaforme di repository di codice come. GitHub

Panoramica di

AWS Security Agent è composto da tre componenti principali:

- Console di gestione AWS: configura gli spazi degli agenti, definisci i requisiti di sicurezza, configura i test di penetrazione, collega repository di codice e gestisci l'accesso degli utenti
- Applicazione Web Security Agent: esegui revisioni progettuali, crea ed esegui modelli di minaccia, esegui test di penetrazione, crea ed esegui revisioni del codice ed esamina i risultati di sicurezza all'interno degli Agent Spaces assegnati
- Integrazione del repository di codice: ricevi revisioni automatiche del codice sulle richieste pull e sulle richieste pull di correzione dei test di penetrazione. Attualmente AWS Security Agent supporta la connessione a GitHub.

Lavori con AWS Security Agent in uno dei tre ruoli, che puoi identificare dall'interfaccia che usi:

Ruolo	Dove lavori e cosa fai
Amministratore	Funziona nella Console di gestione AWS: configura gli Agent Spaces, definisce i requisiti di sicurezza, configura le funzionalità e gestisce l'accesso degli utenti.
Utente	Funziona nell'applicazione Web Security Agent: esegue revisioni di progettaz ione, modelli di minaccia, test di penetrazione e revisioni del codice ed esamina i risultati risultanti.
Sviluppatore	Funziona in GitHub un IDE (come Kiro o Claude Code): riceve risultati di sicurezza automatici su richieste pull ed esegue scansioni del codice senza uscire dall'ambiente di sviluppo.

Utilizziamo questi nomi di ruolo ovunque per indicare chi esegue ogni attività. Una singola persona può ricoprire più di un ruolo.

Configurazione della console

Gli amministratori configurano AWS Security Agent tramite la Console di gestione AWS.

Agent Spaces: quando crei il tuo primo Agent Space nella Console di gestione AWS, AWS Security Agent crea l'applicazione Web per il tuo account. Ogni Agent Space che crei rappresenta un'applicazione o un progetto distinto che desideri proteggere. Nell'applicazione Web, gli utenti selezionano in quale Agent Space lavorare durante le valutazioni di sicurezza.

Requisiti di sicurezza: definisci i requisiti di sicurezza che AWS Security Agent valuta durante la progettazione e le revisioni del codice, organizzati in pacchetti di requisiti di sicurezza. Abilita AWS-managed pacchetti basati sugli standard di settore, crea pacchetti personalizzati per le politiche della tua organizzazione o genera requisiti caricando la documentazione di sicurezza. I requisiti si applicano a tutti gli Agent Spaces.

Configurazione dei test di penetrazione: configura le funzionalità di test di penetrazione per ogni Agent Space mediante:

- Verifica dei domini di destinazione per il test tramite verifica DNS o HTTP
- Configurazione dell'accesso VPC per testare applicazioni private
- Configurazione della CloudWatch registrazione per le esecuzioni dei test di penetrazione
- Configurazione delle funzioni AWS Secrets Manager o Lambda per le credenziali di test
- Specificare i bucket S3 per un contesto applicativo aggiuntivo

Configurazione di revisione del codice: configura le funzionalità di revisione del codice per ogni Agent Space mediante:

- Collegamento di GitHub repository o bucket S3 contenenti codice sorgente
- Selezione delle impostazioni di revisione del codice (vulnerabilità di sicurezza, requisiti personalizzati o entrambi)
- Abilitazione dei commenti pull request per la revisione automatica delle modifiche al codice in GitHub
- Configurazione della CloudWatch registrazione per le esecuzioni di revisione del codice

Configurazione della modellazione delle minacce: configura le funzionalità di modellazione delle minacce per ogni Agent Space mediante:

- Connessione di repository di codice sorgente o bucket S3 contenenti codice sorgente
- Aggiungere documenti di ambito (documenti di progettazione delle funzionalità) per concentrare l'analisi su una funzionalità specifica
- Configurazione della CloudWatch registrazione per le esecuzioni del modello di minaccia
- Configurazione di un ruolo di servizio per l'accesso alle risorse AWS

Integrazioni - Connect gli GitHub archivi a ciascun Agent Space per abilitare le funzionalità chiave:

- Fornisci un contesto applicativo per test di penetrazione più accurati
- Abilita la revisione del codice per scansioni complete del repository e analisi delle pull request
- Abilita la correzione automatica del codice tramite richieste pull per la revisione del codice e i risultati dei test di penetrazione

Accesso utente: gestisci il modo in cui gli utenti accedono all'applicazione Web Security Agent. Se hai abilitato IAM Identity Center (SSO), assegna gli utenti nella console AWS Security Agent per fornire l'accesso SSO diretto all'applicazione Web. Se utilizzi IAM-only access, gli utenti con accesso alla console AWS possono avviare l'applicazione Web tramite il link di accesso amministratore nella Console per qualsiasi Agent Space.

Attività delle applicazioni Web

Gli utenti accedono all'applicazione Web Security Agent per condurre valutazioni di sicurezza all'interno degli Agent Spaces assegnati.

Seleziona Agent Space: quando accedono all'applicazione Web, gli utenti selezionano in quale Agent Space lavorare. Gli utenti possono vedere e accedere solo agli Agent Spaces a cui sono stati assegnati.

Revisioni dei progetti: carica documenti di progettazione e specifiche di architettura per l'analisi rispetto ai requisiti di sicurezza organizzativi. Esamina i risultati con linee guida per la correzione.

Modelli di minaccia: crea ed esegui modelli di minaccia fornendo codice sorgente, documenti tecnici di progettazione (documenti relativi all'ambito) o entrambi. I documenti Scope definiscono su cosa l'agente concentra la sua analisi; il codice sorgente fornisce un contesto sul sistema esistente. Ogni

esecuzione fornisce una panoramica del sistema che descrive l'architettura dell'applicazione, i limiti di affidabilità, i flussi di dati e il livello di sicurezza dell'applicazione, oltre a una serie di minacce classificate per categoria STRIDE con livelli di gravità e consigli pratici.

Revisioni del codice: crea ed esegui revisioni del codice che eseguono analisi statiche complete sull'intero codice sorgente. Seleziona i GitHub repository o le fonti S3, configura le impostazioni di scansione ed esamina i risultati di sicurezza dettagliati con linee guida per la correzione. AWS Security Agent identifica le vulnerabilità di sicurezza e convalida la conformità ai requisiti di sicurezza personalizzati della tua organizzazione nell'intero codebase.

Test di penetrazione: configura ed esegui test di penetrazione fornendo URL di destinazione, dettagli di autenticazione e documentazione. AWS Security Agent esegue test autonomi per scoprire vulnerabilità sfruttabili attraverso scenari di attacco in più fasi.

Esamina i risultati: esamina i risultati di sicurezza dettagliati derivanti da revisioni progettuali, modelli di minaccia, revisioni del codice e test di penetrazione, tra cui analisi dell'impatto, percorsi di attacco riproducibili e linee guida per la risoluzione.

Convalida le correzioni: valutazioni della Re-run sicurezza dopo l'implementazione delle correzioni per verificare che le vulnerabilità siano state risolte.

GitHub integrazione

AWS Security Agent si integra direttamente con GitHub per fornire feedback automatizzati sulla sicurezza nei flussi di lavoro degli sviluppatori.

Commenti sulle richieste pull: dopo che gli amministratori hanno installato l' GitHub app AWS Security Agent e abilitato la revisione del codice con commenti di revisione del codice per un Agent Space, AWS Security Agent analizza automaticamente le richieste pull nei repository collegati. Gli sviluppatori ricevono i risultati di sicurezza e le linee guida per la correzione direttamente nei commenti delle pull request, che convalidano le modifiche al codice rispetto ai requisiti di sicurezza organizzativi e alle vulnerabilità comuni.

Riparazione automatica: quando gli utenti abilitano la correzione automatica del codice per una revisione del codice, AWS Security Agent genera correzioni per le vulnerabilità identificate e invia richieste pull ai repository associati. GitHub

Correzione dei test di penetrazione: quando gli amministratori abilitano la risoluzione dei problemi nella console, gli utenti possono richiedere la correzione automatica dei risultati dei test di

penetrazione dall'applicazione Web. AWS Security Agent apre una pull request al GitHub repository associato con correzioni di codice per risolvere la vulnerabilità.

Comprendi la gerarchia e il ciclo di vita delle risorse

AWS Security Agent organizza le risorse per i test di sicurezza in una struttura gerarchica che determina ciò che è condiviso all'interno dell'organizzazione e l'ambito per applicazione. La comprensione di questa struttura ti aiuta a configurare AWS Security Agent in modo efficace e a sapere dove trovare e gestire diverse risorse.

Cosa viene condiviso all'interno della tua organizzazione

Alcune risorse in AWS Security Agent vengono configurate una sola volta a livello organizzativo e si applicano a tutte le applicazioni e gli Agent Spaces. Queste risorse a livello di tenant garantiscono coerenza e riducono il lavoro di configurazione duplicato.

Risorsa	In cosa consiste	Perché è condivisa
Requisiti di sicurezza	Standard di sicurezza organizzativi che definiscono ciò che AWS Security Agent convalida durante la progettazione e le revisioni del codice	Le tue policy di sicurezza si applicano a tutte le applicazioni. Definiscili una sola volta e AWS Security Agent li applica ovunque.
GitHub integrazioni	GitHub Organizzazioni o account utente registrati autorizzati a connettersi con AWS Security Agent	Registra la tua GitHub organizzazione una sola volta, quindi collega repository specifici a qualsiasi Agent Space, se necessario.
Configurazioni IAM Identity Center	Impostazioni SSO che controllano il modo in cui gli utenti accedono ad AWS Security Agent	La gestione centralizzata delle identità si applica a tutti gli Agent Spaces dell'organizzazione.

> **Important**
>
> Le modifiche ai requisiti di sicurezza influiscono su tutte le future revisioni progettuali e le revisioni del codice in tutti gli Agent Spaces. Le recensioni esistenti non sono interessate.

Cosa rientra nell'ambito di Agent Space

Ogni Agent Space rappresenta un'applicazione o un progetto distinto che si desidera proteggere. Le risorse a livello di Agent Space sono destinate a quell'applicazione specifica, consentendo a diversi team di lavorare in modo indipendente con le proprie configurazioni e valutazioni.

Risorsa	In cosa consiste	Perché è suddiviso in base all'appli cazione
Configura zioni dei test di penetrazione	Esegui il test delle configurazioni per caratteristiche, endpoint API o funzionalità specifici all'interno dell'applicazione	Ogni applicazione ha obiettivi, metodi di autenticazione e limiti di ambito unici specifici per tale applicazione.
Revisioni dei progetti	Valutazioni individuali della sicurezza architettonica dei documenti di progettazione	Ogni applicazione ha i propri documenti di architettura e progettaz ione che vengono valutati in modo indipendente.
Modelli di minaccia	Valutazioni di modellizzazione delle minacce che creano una panoramica del sistema e identificano le minacce dal codice sorgente, dai documenti di progettazione o da entrambi	Ogni applicazione ha il proprio codice e il proprio design ed è modellata in modo indipendente sulle minacce. I modelli di minaccia sono configura zioni riutilizzabili che è possibile rieseguire man mano che il codice e il design si evolvono.
Integrazioni	Fornitori di sorgenti e documenta zione (GitHub GitLab, Bitbucket , GitHub Enterprise Server e Confluence) collegati a questo Agent Space	Applicazioni diverse si basano su fonti e documentazione diverse. La loro connessione a livello di Agent Space mantiene chiari i confini delle applicazioni.
Impostazioni di revisione del codice	Configurazione delle funzionalità di revisione del codice, tra cui sorgenti connesse, impostazioni di scansione e abilitazione dei commenti PR	Ogni applicazione ha i propri repository e le esigenze di revisione della sicurezza devono essere configurate in modo indipendente.

Risorsa	In cosa consiste	Perché è suddiviso in base all'appli cazione
Impostazioni di correzione dei test di penetrazi one	Configurazione di quali repository collegati possono ricevere richieste automatiche di fix pull per i risultati dei test di penetrazione	I team controllano dove AWS Security Agent può inviare modifiche al codice in base al flusso di lavoro dell'applicazione.
Assegnazioni degli utenti	Utenti che hanno accesso a questo specifico Agent Space	I team visualizzano solo le valutazio ni di sicurezza per le applicazioni di cui sono responsabili, in modo da mantenere il lavoro organizzato e concentrato.

> **Tip**
>
> Consigliamo di creare un Agent Space per applicazione o progetto per mantenere confini chiari tra i team e organizzare le valutazioni della sicurezza in modo efficace.

In che modo i GitHub repository si inseriscono nella gerarchia

GitHub i repository sono integrati attraverso un processo in più fasi che collega le risorse organizzative a applicazioni specifiche:

1. Registrazione a livello di tenant: autorizza l' GitHub app AWS Security Agent per la tua GitHub organizzazione o il tuo account utente una sola volta
2. Connetti a livello di Agent Space: seleziona repository specifici per connetterti a ogni Agent Space
3. Configura l'utilizzo per repository: abilita funzionalità specifiche per ogni repository connesso:
   - Revisione del codice: scansione completa del codice sorgente e analisi automatica delle pull request
   - Contesto dei test di penetrazione: comprensione dell'applicazione dal codice sorgente durante i test di penetrazione
   - Correzione automatica del codice: pull request automatizzate con correzioni di vulnerabilità per la revisione del codice e i risultati dei test di penetrazione

Un singolo repository può essere collegato a più Agent Spaces con funzionalità diverse abilitate in ciascuno di essi.

Principali differenze tra le funzionalità di sicurezza

Ogni funzionalità di sicurezza in AWS Security Agent segue un modello di flusso di lavoro diverso in base a come viene utilizzata dai team di sicurezza.

Test di penetrazione: configurazioni riutilizzabili con esecuzioni indipendenti

I test di penetrazione utilizzano un modello di configurazione ed esecuzione che supporta test di sicurezza iterativi:

- Crea una sola volta, esegui più volte: definisci una configurazione per un obiettivo specifico (endpoint API, area delle funzionalità) con limiti di ambito, autenticazione e parametri di test
- Esecuzioni indipendenti: esegui la stessa configurazione più volte per migliorare la sicurezza. Ogni esecuzione è indipendente e genera nuove scoperte

Questo modello supporta la convalida continua della sicurezza durante lo sviluppo e l'implementazione di miglioramenti.

Revisioni dei progetti: One-off valutazioni con clonazione

Le revisioni dei progetti sono valutazioni indipendenti che non seguono un modello di configurazione riutilizzabile:

- Valutazione singola: ogni revisione del progetto analizza una volta i documenti caricati rispetto ai requisiti di sicurezza dell'organizzazione
- Impossibile rieseguire: le revisioni dei progetti non sono riutilizzabili. Non è possibile eseguire nuovamente la stessa revisione
- Clona per gli aggiornamenti: clona una revisione del progetto esistente per creare una nuova revisione con i documenti originali precaricati, in modo da aggiornare i documenti ed eseguire una nuova analisi

Questo modello supporta valutazioni della sicurezza architetturale point-in-time.

Revisioni del codice: configurazioni riutilizzabili con scansioni su richiesta e analisi PR automatica

Le revisioni del codice forniscono due modalità operative per proteggere il codice sorgente:

- Revisioni complete del codice (applicazione web): crea configurazioni di revisione del codice che selezionano GitHub repository o sorgenti S3, quindi esegui scansioni complete su richiesta. Ogni esecuzione esegue analisi statiche sull'intero codice sorgente e genera risultati con indicazioni sulla correzione. È possibile eseguire nuovamente la stessa configurazione di revisione del codice man mano che il codice si evolve.
- Pull request comments (GitHub): abilita l'analisi automatizzata per i repository connessi GitHub . AWS Security Agent esamina automaticamente le richieste pull quando sono contrassegnate come pronte per la revisione e pubblica i risultati di sicurezza come commenti direttamente in GitHub.

Entrambe le modalità utilizzano le impostazioni di revisione del codice configurate (vulnerabilità di sicurezza, requisiti personalizzati o entrambi) e supportano la correzione automatica del codice tramite richieste pull.

Modelli di minaccia: configurazioni riutilizzabili con esecuzioni su richiesta

I modelli di minaccia utilizzano un modello di configurazione ed esecuzione che supporta la valutazione iterativa dell'architettura:

- Crea una sola volta, esegui più volte: definisci un modello di minaccia selezionando il codice sorgente come origine, caricando i documenti di progettazione come documenti di riferimento o entrambi. Eseguilo su richiesta e rieseguilo man mano che il codice e il design si evolvono.
- Input flessibili: esegui un modello di minaccia solo sul codice sorgente, solo sui documenti di progettazione o su entrambi. I documenti Scope definiscono su cosa l'agente concentra la sua analisi; il codice sorgente fornisce un contesto sul sistema esistente.
- Panoramica del sistema e minacce: ogni esecuzione fornisce una panoramica del sistema che descrive l'architettura, i limiti di affidabilità, i flussi di dati e il livello di sicurezza dell'applicazione, oltre a una serie di minacce classificate per categoria STRIDE con gravità, prove e raccomandazioni attuabili.

Comprendere le relazioni tra le risorse

La gerarchia determina dove configurare e accedere a diverse risorse:

Nella Console di gestione AWS:

- Configura le risorse a livello di tenant (requisiti di sicurezza, GitHub integrazioni, IAM Identity Center)
- Crea e gestisci Agent Spaces
- Configura le impostazioni di Agent Space (repository connessi, attivazione della revisione del codice, correzione dei test di penetrazione)

Nell'applicazione Web Security Agent:

- Crea e gestisci configurazioni ed esecuzioni di test di penetrazione
- Crea e gestisci le revisioni dei progetti
- Crea, gestisci ed esegui revisioni del codice su repository connessi e sorgenti S3
- Crea, gestisci ed esegui modelli di minaccia sulla base del codice sorgente, dei documenti di ambito o di entrambi
- Visualizza i risultati dei test di penetrazione, delle revisioni del codice, delle revisioni della progettazione e dei modelli di minaccia

In GitHub:

- Visualizza i risultati della revisione del codice pull request come commenti di pull request
- Ricevi richieste pull di correzione automatizzate per la revisione del codice e i risultati dei test di penetrazione (se abilitate nell'Agent Space)

> **Note**
>
> I risultati della revisione del codice delle pull request vengono visualizzati in. GitHub I risultati completi della revisione del codice, del test di penetrazione e della revisione del progetto vengono visualizzati nell'applicazione Web Security Agent.

Nozioni di base

Iscriviti, trova il punto di partenza giusto per il tuo obiettivo ed esegui la tua prima valutazione con un Quickstart.

Iscriviti per un AWS account

Per iniziare AWS, hai bisogno di un AWS account. Per informazioni sulla creazione di un AWS account, consulta Guida introduttiva a un AWSAWS account nella Guida di riferimento alla gestione degli account.

Scegli il tuo percorso

Trova il punto di partenza giusto per ciò che vuoi fare con AWS Security Agent. Utilizza la tabella seguente per abbinare il tuo obiettivo a un'attività, quindi vai direttamente a quella pagina. Se non conosci AWS Security Agent, leggi the section called "Cos'è AWS Security Agent?" prima per una rapida panoramica.

Voglio...	Chi	Inizia da qui
Scopri cosa fa AWS Security Agent prima di configurarlo	Tutti	the section called "Cos'è AWS Security Agent?"
Configura il servizio e crea uno spazio per agenti	Admin	the section called "Configurazione di AWS Security Agent"
Testa la mia applicazione live o distribuita per individuare eventuali vulnerabilità sfruttabili	Utente	the section called "Avvio rapido: esegui un test di penetrazione"
Scansiona il mio codice sorgente per individuare vulnerabilità e violazioni delle policy	Utente	the section called "Quickstart: Esegui una revisione del codice"
Modella in che modo la mia applicazione potrebbe essere attaccata (STRIDE)	Utente	the section called "Quickstart: Esegui un modello di minaccia"

Voglio...	Chi	Inizia da qui
Ottieni feedback sulla sicurezza di un progetto prima di scrivere codice	Utente	the section called "Crea una revisione del design"
Scansiona il codice senza uscire dal mio IDE (Kiro o Claude Code)	Developer	the section called "Esegui scansioni di sicurezza del codice dal tuo IDE"
Scansiona solo le mie righe modificate prima di unirle	Developer	the section called "Esegui una scansione del codice differenziale con S3"
Ricevi commenti di sicurezza automatici sulle richieste pull e sulle richieste di unione	Admin	the section called "Abilita la revisione del codice"
Esamina i risultati e decidi cosa correggere prima	Utente	Test di penetrazione, revisione del codice, modello di minaccia, revisione del progetto

> **Note**
>
> AWS Security Agent utilizza tre ruoli, che puoi identificare dall'interfaccia in cui lavori: l'amministratore lavora nella Console di gestione AWS (configurazione e configurazione), l'utente lavora nell'applicazione Web (esegue valutazioni e revisione dei risultati) e lo sviluppatore lavora in un IDE come Kiro GitHub o Claude Code. Una singola persona può ricoprire più di un ruolo. Per le definizioni complete, vederethe section called "Come funziona AWS Security Agent".

Avvio rapido: esegui un test di penetrazione

Questa guida introduttiva ti guida nell'esecuzione del tuo primo penetration test (pentest) con AWS Security Agent. Un test di penetrazione analizza l'applicazione distribuita su un dominio di destinazione verificato e restituisce i risultati di sicurezza, ciascuno con un indice di gravità e prove a supporto. Copre un'applicazione accessibile al pubblico; per testarne una ospitata in un VPC privato, vedi. the section called "Abilita il test di penetrazione"

> **Note**
>
> È necessario accedere alla Console di gestione AWS per configurare AWS Security Agent e definire l'ambito del test e accedere all'applicazione Web per creare ed eseguire test di penetrazione.

Prerequisiti

Prima di iniziare, assicurati di avere:

- Accesso alla Console di gestione AWS con le autorizzazioni per configurare AWS Security Agent.
- Un dominio di destinazione attivo che ospita l'applicazione che desideri testare.
- La possibilità di aggiungere un record DNS per quel dominio o una zona ospitata da Route 53 nello stesso account AWS, in modo da poter verificare la proprietà.
- (Facoltativo) Un repository di codice sorgente (GitHubo Bitbucket) per la tua applicazione, per fornire all'agente un contesto più approfondito. GitLab

Fase 1: configurare AWS Security Agent nella console AWS

Se non hai ancora configurato AWS Security Agent, completa la configurazione iniziale:

1. Accedi ad AWS Security Agent nella Console di gestione AWS.
2. Seleziona Configura AWS Security Agent.
3. Crea uno spazio per agenti. Uno spazio agente può essere utilizzato da più utenti e deve essere specifico per ogni applicazione che si desidera testare. Inserisci un nome e una descrizione. Il nome deve identificare l'applicazione per la quale si desidera eseguire il penetration test.
4. Seleziona IAM-only l'accesso in Configurazione dell'accesso utente.
   - Questo quickstart non copre l'abilitazione del Single Sign-On (SSO) con IAM Identity Center, che consente agli utenti di accedere all'applicazione Web direttamente dalla console AWS.
   - Per consentire agli utenti senza accesso alla Console di gestione AWS di avviare i test di penetrazione, abilita l'integrazione con IAM Identity Center. Per informazioni dettagliate, vedi the section called "Concedi agli utenti l'accesso all'app Web AWS Security Agent".
5. Scegli Configura AWS Security Agent.

> **Note**
>
> Quando scegli Configurazione, AWS Security Agent crea il tuo Agent Space e stabilisce un'applicazione Web in cui gli utenti possono eseguire test di penetrazione, revisioni del codice, modelli di minaccia e revisioni del progetto.

Passaggio 2: abilita i test di penetrazione e verifica il tuo dominio

> **Note**
>
> Nella console AWS definisci l'ambito di ciò che può essere testato. Gli utenti eseguono quindi test di penetrazione specifici all'interno di tale ambito dall'applicazione Web.

1. Dalla barra laterale sinistra, seleziona Agent Spaces, quindi seleziona l'Agent Space che hai creato nel passaggio 1.
2. Seleziona la scheda Penetration test, quindi scegli Configura test di penetrazione per aprire la procedura guidata.
3. Configura dominio: inserisci il dominio di destinazione che desideri testare e seleziona un metodo di verifica, DNS TXT Record o HTTP Route. Il dominio deve essere attivo e ospitare l'applicazione che desideri testare. Scegli Next (Successivo).
4. Verifica domini: verifica la proprietà di ogni dominio nella tabella Domini di Target. AWS Security Agent esegue test solo su domini verificati. Per i passaggi dettagliati e i valori esatti da copiare, consultathe section called "Abilita un dominio applicativo per i test di penetrazione".
   - Domini Route 53 nello stesso account AWS: seleziona il dominio e scegli la One-click verifica. AWS Security Agent crea il record DNS e completa la verifica per te.
   - Record DNS TXT (altri provider DNS): nella tabella Domini di Target, copia il nome del record e il valore del record, aggiungili come record TXT con il tuo provider DNS, quindi seleziona il dominio e scegli Verifica. La propagazione delle modifiche DNS può richiedere del tempo, pertanto la verifica potrebbe non essere completata immediatamente.
   - Percorso HTTP: crea un file su **`.well-known/aws/securityagent-domain-verification.json`** sul tuo server web, aggiungi il token di verifica nel formato**`{"tokens": ["<token>"]}`**, quindi seleziona il dominio e scegli Verifica.

5. (Facoltativo) Configura funzionalità aggiuntive: aggiungi risorse opzionali come gruppi di CloudWatch log e credenziali. La sezione Accesso al servizio è preconfigurata: AWS Security Agent crea un ruolo di servizio con le autorizzazioni richieste a meno che non si scelga un ruolo IAM esistente.

Fase 3: Connect il codice sorgente (opzionale)

La connessione a un provider di codice sorgente fornisce ad AWS Security Agent un contesto sulla tua applicazione e migliora la copertura dei test di penetrazione. Questa fase è facoltativa.

1. Nella scheda Penetration test, scegli Aggiungi sul banner Connect a source code provider for penetration testing nella parte superiore della pagina.
2. Registrati e collega il tuo provider, quindi seleziona gli archivi da rendere disponibili per i test di penetrazione.

Per il flusso di integrazione completo, consulta Connect AWS Security Agent ai GitHub repository o l'argomento Connect per il tuo provider.

Fase 4: Creare ed eseguire un test di penetrazione

> **Note**
>
> Crei ed esegui test di penetrazione nell'applicazione web AWS Security Agent. Consigliamo di eseguire i test in un ambiente di test che rispecchi fedelmente la produzione.

1. Avvia l'applicazione Web: seleziona la scheda App Web, quindi Accesso amministratore.
2. Nella barra laterale sinistra, scegli Test di penetrazione, quindi Crea un test di penetrazione.
3. Dettagli del test di penetrazione: imposta l'ambito del test e la fonte del registro:
   a. Inserisci un nome Pentest.
   b. In Target URLs, seleziona o inserisci un dominio verificato da testare (ad esempio,`https://example.com`). È possibile testare solo i domini verificati e i sottodomini vengono coperti automaticamente.
   c. (Facoltativo) In URL accessibili, aggiungi i domini che l'agente deve raggiungere per l'accesso e la navigazione ma che non deve attaccare, come provider di identità, CDN o API esterni al

dominio di destinazione. AWS Security Agent può raggiungere questi domini ma non li testa; vengono attaccati solo i domini di destinazione.

d. Esamina le regole di configurazione della rete per confermare quali endpoint possono e non possono ricevere traffico durante il test.

e. In Autorizzazioni, seleziona un ruolo di servizio e, facoltativamente, un gruppo di log. CloudWatch Scegli Next (Successivo).

4. (Facoltativo) Risorse VPC: configura un VPC se la destinazione si trova su una rete privata non raggiungibile pubblicamente. Per informazioni, consulta the section called "Abilita il test di penetrazione".
5. (Facoltativo) Risorse per l'autenticazione: fornisci le credenziali in modo che l'agente possa raggiungere percorsi autenticati e non pubblici. Ti consigliamo di aggiungerle per ampliare la copertura e far emergere le vulnerabilità dietro un accesso.
6. (Facoltativo) Configurazione aggiuntiva: aggiungi contesti applicativi come file, GitHub repository o fonti S3 per migliorare la qualità delle ricerche. Puoi anche abilitare la correzione automatica del codice e impostare altre opzioni di esecuzione qui.
7. Scegli Crea ed esegui per iniziare subito il test o Crea pentest per salvarlo ed eseguirlo in un secondo momento.

Fase 5: Rivedi i risultati del test di penetrazione

1. Il completamento di un test di penetrazione può richiedere diverse ore. Il più completo entro 16 ore, a seconda delle dimensioni e della complessità dell'applicazione.
2. L'esecuzione inizia con una fase di Preflight che convalida la configurazione prima dell'inizio del test: configura l'infrastruttura di registrazione, verifica che gli endpoint di destinazione siano raggiungibili e prepara l'ambiente di test. Se un controllo di preflight fallisce (ad esempio, un dominio di destinazione che non può essere risolto), l'esecuzione si interrompe prima dell'inizio del test. Apri la scheda Preflight per vedere quale controllo non è riuscito, risolvilo e inizia una nuova esecuzione.
3. Al termine dell'esecuzione, aprila e consulta le schede Run overview, Logs e Findings.
4. Nella scheda Risultati, seleziona un risultato per visualizzarne la descrizione, la gravità, il tipo di rischio e le prove a supporto.

Per ulteriori dettagli, consulta the section called "Crea un test di penetrazione" e the section called "Esamina i risultati di un test di penetrazione".

Quickstart: Esegui una revisione del codice

Questa guida introduttiva illustra come eseguire la prima revisione del codice con AWS Security Agent. AWS Security Agent analizza i tuoi repository di codice sorgente alla ricerca di vulnerabilità di sicurezza e conformità ai requisiti di sicurezza della tua organizzazione.

> **Note**
>
> È necessario accedere alla Console di gestione AWS per configurare AWS Security Agent e accedere all'applicazione Web per creare ed eseguire revisioni del codice.

Prerequisiti

Prima di iniziare, assicurati di avere:

- Accesso alla Console di gestione AWS con le autorizzazioni per configurare AWS Security Agent.
- Un repository di codice sorgente (GitHub GitLab, o Bitbucket) o un codice sorgente Amazon S3 che contiene il codice che desideri esaminare.

Fase 1: configurare AWS Security Agent nella console AWS

Se non hai ancora configurato AWS Security Agent, completa la configurazione iniziale:

1. Accedi ad AWS Security Agent nella Console di gestione AWS.
2. Seleziona Configura AWS Security Agent.
3. Crea uno spazio per agenti. Uno spazio agente può essere utilizzato da più utenti e deve essere specifico per ogni applicazione che si desidera testare. Inserisci un nome e una descrizione per il tuo primo spazio agente. Questo nome viene visualizzato agli utenti nell'applicazione Web. Il nome deve identificare l'applicazione di cui si desidera esaminare il codice.
4. Seleziona IAM-only l'accesso in Configurazione dell'accesso utente.
   - Questo quickstart non copre l'abilitazione del Single Sign-On (SSO) con IAM Identity Center. Ciò consente agli utenti di accedere direttamente all'applicazione Web AWS Security Agent dalla console AWS.

- Per consentire agli utenti senza la Console di gestione AWS di accedere a eseguire revisioni del codice, abilita l'integrazione con IAM Identity Center. Per informazioni dettagliate, vedi the section called "Concedi agli utenti l'accesso all'app Web AWS Security Agent".

5. Scegli Configura AWS Security Agent.

> **Note**
>
> Quando scegli Configurazione, AWS Security Agent crea il tuo Agent Space e stabilisce un'applicazione Web in cui gli utenti possono eseguire test di penetrazione, revisioni del codice, modelli di minaccia e revisioni del progetto.

Fase 2: abilitare e configurare la revisione del codice

> **Note**
>
> Se disponi già di GitHub repository o bucket S3 collegati a Agent Space (ad esempio, tramite la configurazione dei test di penetrazione), la revisione del codice è già abilitata. Puoi saltare questo passaggio e andare direttamente all'applicazione web.

Apri la procedura guidata di configurazione per la revisione del codice

1. Dalla barra laterale sinistra, seleziona Agent Spaces, quindi seleziona Agent Space.
2. Seleziona Abilita la revisione del codice dall'intestazione o dalla scheda Revisione del codice.

Connect integrazioni, repository e bucket

1. (Se non hai ancora un' GitHub integrazione) Crea una registrazione. GitHub Se ne hai già una, vai al passaggio successivo.
   a. Nella sezione Integrazioni connesse, scegli Aggiungi e poi Crea nuova registrazione.
   b. Seleziona GitHube scegli Avanti.
   c. Scegli Installa e autorizza, quindi completa l'installazione in GitHub:
      i. Seleziona l' GitHub utente o l'organizzazione proprietaria del repository che desideri esaminare.

ii. Seleziona Tutti i repository o Seleziona solo i repository.

iii. Scegli Installa e autorizza e completa l'autenticazione. GitHub

d. Tornando alla Console di gestione AWS, inserisci un nome di registrazione e conferma che il tipo di account corrisponde a quello in cui hai installato l' GitHub app.

e. Scegli Connect per salvare la registrazione.

Per il flusso di GitHub integrazione completo, consulta Connect AWS Security Agent ai GitHub repository.

2. Connect i GitHub repository. Nella sezione Integrazioni connesse, scegli Aggiungi, quindi seleziona la tua GitHub registrazione. Viene visualizzata la GitHub procedura guidata Connect in due passaggi:

a. In Connect GitHub repositories, seleziona i repository da includere e scegli Avanti.

b. In Gestisci le funzionalità, attiva le seguenti opzioni per repository:

- Commenti sulla revisione del codice: consenti ad AWS Security Agent di pubblicare i risultati di sicurezza come commenti sulle richieste pull nel repository.
- Correzione automatica: consenti agli utenti dell'applicazione Web AWS Security Agent di richiedere richieste di recupero per correggere i risultati.

c. Scegli Salva per tornare alla procedura guidata di configurazione.

3. (Opzionale) Connect sorgenti S3. Nella sezione bucket S3, scegli Aggiungi risorsa S3 e inserisci l'URI S3 per un bucket contenente il codice sorgente, oppure scegli Sfoglia per sceglierne uno.

4. Seleziona le impostazioni di revisione del codice. L'impostazione predefinita, Security requirements and vulnerability findings, analizza il codice sia per verificarne la conformità ai requisiti di sicurezza abilitati che le vulnerabilità comuni.

5. Scegli Next (Successivo).

Configurazioni facoltative

1. Configura i gruppi di CloudWatch log e l'accesso ai servizi opzionali. Il ruolo di servizio predefinito è preconfigurato con le autorizzazioni richieste.

2. Scegli Save (Salva).

Passaggio 3: Creare ed eseguire una revisione del codice

> **Note**
>
> Puoi creare ed eseguire revisioni del codice solo nell'applicazione Web AWS Security Agent.

1. Seleziona la scheda App Web e quindi Accesso amministratore per avviare l'applicazione Web AWS Security Agent.
2. Nella barra laterale sinistra, scegli Code reviews.
3. Scegli Crea revisione del codice.
4. Configura la revisione del codice:
   a. Inserisci un titolo che identifichi l'ambito di questa revisione (ad esempio, «billing-service-security-review»).
   b. In Sorgenti, seleziona i GitHub repository che hai collegato a Agent Space nel passaggio 2 o inserisci le fonti S3 che desideri scansionare.
   c. Seleziona il ruolo Service tra i ruoli configurati.
   d. (Facoltativo) Seleziona Abilita la correzione automatica del codice per fare in modo che AWS Security Agent invii automaticamente richieste pull con correzioni per tutti i risultati.
5. Scegli Create code review.
6. Nella pagina dei dettagli della revisione del codice, scegli Inizia revisione.

Fase 4: Rivedi i risultati della revisione del codice

1. La revisione del codice richiede in genere 30-60 minuti a seconda delle dimensioni della codebase.
2. L'esecuzione inizia con una fase di Preflight che convalida la configurazione prima dell'inizio della scansione: conferma che AWS Security Agent è in grado di estrarre il codice sorgente dal repository o dalla sorgente S3 e configura l'ambiente di scansione. Se un controllo di preflight fallisce (ad esempio, non può accedere alla fonte), l'esecuzione si interrompe prima dell'analisi statica. Apri la scheda Preflight per vedere quale controllo non è riuscito, risolvilo e inizia una nuova esecuzione.
3. Una volta completata, vai all'esecuzione completata e seleziona la scheda Findings.
4. Esamina i risultati nella visualizzazione dettagliata dell'elenco:
   a. Seleziona un risultato dal pannello di sinistra per visualizzarne i dettagli.

b. Consulta le sezioni Descrizione, Posizioni dei codici, Evidenza e Correzione consigliata.
c. Usa il codice Remediate per generare una pull request con una correzione o rivedi i PR di riparazione automatici se hai abilitato questa opzione.

Per ulteriori dettagli, consulta the section called "Creare una revisione del codice" e the section called "Esamina i risultati di una revisione del codice".

Quickstart: Esegui un modello di minaccia

Questa guida introduttiva ti guida nell'esecuzione del tuo primo modello di minaccia con AWS Security Agent. Un modello di minaccia analizza l'architettura dell'applicazione e produce una panoramica del sistema (come AWS Security Agent comprende il sistema) e una serie di minacce (come potrebbe essere attaccata, ciascuna con un livello di gravità, una classificazione STRIDE e raccomandazioni). Puoi eseguire un modello di minaccia sui documenti di progettazione (documenti di ambito) per definire l'obiettivo, sul codice sorgente (fonti) per fornire un contesto sul sistema esistente, o entrambi.

> **Note**
>
> È necessario accedere alla Console di gestione AWS per configurare AWS Security Agent e accedere all'applicazione Web per creare ed eseguire modelli di minaccia.

Fase 1: configurare AWS Security Agent nella console AWS

Se non hai ancora configurato AWS Security Agent, completa la configurazione iniziale:

1. Accedi ad AWS Security Agent nella Console di gestione AWS.
2. Seleziona Configura AWS Security Agent.
3. Crea uno spazio per agenti. Uno spazio agente può essere utilizzato da più utenti e deve essere specifico per ogni applicazione che desideri proteggere. Inserisci un nome e una descrizione per il tuo primo spazio agente. Il nome deve identificare l'applicazione che desideri minacciare.
4. Seleziona IAM-only l'accesso in Configurazione dell'accesso utente.
   - Questo quickstart non copre l'abilitazione del Single Sign-On (SSO) con IAM Identity Center. Ciò consente agli utenti di accedere direttamente all'applicazione Web AWS Security Agent dalla console AWS.

- Se desideri consentire agli utenti senza accesso alla Console di gestione AWS di eseguire attività come l'avvio di un modello di minaccia, devi abilitare l'integrazione con IAM Identity Center.

5. Scegli Configura AWS Security Agent.

> **Note**
>
> Quando scegli Configurazione, AWS Security Agent crea il tuo Agent Space e stabilisce un'applicazione Web in cui gli utenti possono eseguire test di penetrazione, revisioni del codice, modelli di minaccia e revisioni del progetto.

Fase 2: Connect il codice sorgente

> **Note**
>
> Se disponi già di repository o bucket S3 collegati a Agent Space (ad esempio, tramite la revisione del codice o la configurazione dei test di penetrazione), puoi saltare questo passaggio e passare direttamente all'applicazione web. Puoi sempre eseguire un modello di minaccia sui documenti di ambito caricati senza collegare alcun codice sorgente.

Connect repository o bucket S3 che contengono il codice sorgente che desideri che l'agente utilizzi come contesto per comprendere il tuo sistema esistente:

1. Dalla barra laterale sinistra, seleziona Agent Spaces, quindi seleziona Agent Space.
2. Vai alla sezione Integrazioni per connettere il tuo fornitore di codice sorgente.
3. In alternativa, collega i bucket S3 che contengono il codice sorgente.

Per il flusso di integrazione completo, consulta Connect AWS Security Agent ai GitHub repository.

Fase 3: Creare ed eseguire un modello di minaccia

> **Note**
>
> Puoi creare ed eseguire modelli di minaccia nell'applicazione web AWS Security Agent.

1. Avvia l'applicazione Web dalla scheda App Web nella Console di gestione AWS. In alternativa, se hai configurato IAM Identity Center, accedi direttamente.
2. Nella barra laterale sinistra, scegli Threat models.
3. Scegli Crea modello di minaccia.
4. Configura il modello di minaccia:
   a. Inserisci un titolo che identifichi l'ambito di questo modello di minaccia (ad esempio, «billing-service» o «checkout-api»).
   b. Fornisci almeno un input:
      - In Scope docs, carica documenti di progettazione (DOC, DOCX, JPEG, MD, PDF, PNG o TXT), inserisci gli URI S3 o seleziona le pagine Confluence.
      - In Sorgenti, seleziona i repository dalle integrazioni connesse o inserisci gli URI S3 contenenti il codice sorgente.

      > **Tip**
      >
      > Fornisci sia i sorgenti che i documenti relativi all'ambito per adattare il modello di minaccia a un progetto specifico (ad esempio, un documento sulla progettazione delle funzionalità) fornendo al contempo all'agente il codice sorgente come contesto per comprendere il sistema esistente.

   c. Seleziona il ruolo di servizio tra i ruoli configurati.
   d. (Facoltativo) Seleziona un gruppo di log per CloudWatch i log.
5. Scegli Crea modello di minaccia.
6. Nella pagina dei dettagli del modello di minaccia, scegli Avvia esecuzione.

Fase 4: Analizza le minacce

1. L'esecuzione procede attraverso le sue attività di analisi. È possibile monitorare l'avanzamento nella scheda Preflight e visualizzare i dettagli delle attività nella scheda Registri.
2. Una volta completata, lo stato dell'esecuzione diventa Completato.
3. Seleziona la scheda Panoramica per visualizzare la panoramica del sistema e la distribuzione della gravità.
4. Seleziona la scheda Minacce per esaminare le minacce identificate:
   a. Seleziona una minaccia dall'elenco per visualizzarne i dettagli nel pannello laterale.

b. Consulta le categorie Dichiarazione, Severità, STRIDE, Raccomandazione, Evidenza e altri campi.
c. Aggiorna lo stato della minaccia su Risolta o Ignorata man mano che affronti o classifichi ciascuna minaccia.

Per ulteriori dettagli, consulta the section called "Crea un modello di minaccia" e the section called "Esamina le minacce partendo da un modello di minaccia".

Per amministratori (console)

In qualità di amministratore, configuri AWS Security Agent nella Console di gestione AWS e configuri Agent Spaces a cui gli utenti accedono tramite l'applicazione Web AWS Security Agent. Ogni Agent Space rappresenta un ambiente distinto con autorizzazioni e risorse specifiche.

Ti consigliamo di creare un Agent Space unico per ogni applicazione che desideri testare. Ad esempio, se hai due progetti interni, un'applicazione di fatturazione e un'applicazione di tracciamento delle attività, dovresti creare due Agent Spaces separati.

Configurazione di esempio

Prendi in considerazione la possibilità che un amministratore configuri un Agent Space per valutare la sicurezza di un'applicazione di fatturazione interna. L'amministratore dovrebbe:

- Verificare il dominio (ad esempio`beta.billing.example.com`)
- Connect GitHub e abilita la revisione del codice
- Configura l'accesso alla rete assegnando un VPC, una sottorete e un gruppo di sicurezza appropriati per i test di penetrazione

Quando gli utenti avviano un penetration test o una revisione del progetto, possono scegliere tra queste risorse preconfigurate, lavorare entro i limiti che avete definito e allo stesso tempo mantenere la flessibilità necessaria per le loro esigenze di valutazione specifiche.

Configurazione e creazione di Agent Spaces

Configura AWS Security Agent per la tua organizzazione e crea gli Agent Spaces che coprono le risorse e le valutazioni di ciascuna applicazione.

Configurazione di AWS Security Agent

Configura AWS Security Agent per la tua organizzazione creando il tuo primo Agent Space e stabilendo in che modo gli utenti accederanno all'applicazione web.

Questa configurazione iniziale consente agli amministratori di configurare le funzionalità di sicurezza nella console AWS e fornisce agli utenti l'accesso alla revisione del progetto e ai test di penetrazione

tramite l'applicazione Web Security Agent. Dopo questa configurazione unica, puoi creare Agent Spaces aggiuntivi con un processo semplificato.

Panoramica di

Comprendere Agent Spaces

Un Agent Space è uno spazio di lavoro dedicato per proteggere un'applicazione o un progetto specifico. Contiene tutte le revisioni di sicurezza, gli GitHub archivi opzionalmente collegati, le configurazioni dei test di penetrazione, i risultati e i risultati per quell'applicazione.

Agent Spaces ti aiuta a organizzare il lavoro di sicurezza mantenendo separate le valutazioni di sicurezza di ciascuna applicazione, permettendo ai team di concentrarsi sulla propria applicazione specifica. Ti consigliamo di creare un Agent Space per applicazione o progetto per mantenere confini chiari.

I requisiti di sicurezza sono definiti a livello di organizzazione e si applicano a tutti gli Agent Spaces, mentre ogni Agent Space conserva i propri documenti di progettazione, archivi di codice, configurazioni dei test di penetrazione, risultati dei test di penetrazione e risultati di sicurezza.

Cosa è incluso in un Agent Space

Ogni Agent Space contiene:

- GitHub Repository opzionalmente collegati associati all'applicazione o al progetto
- Revisioni precedenti del progetto dell'applicazione
- Configurazioni e limiti dei test di penetrazione specifici dell'applicazione
- Risultati dei test di penetrazione e risultati di sicurezza

Cosa configurerai durante la configurazione

Durante questa prima configurazione, prenderai decisioni organizzative che si applicano a tutti gli Agent Spaces:

- Metodo di accesso: scegli in che modo gli utenti accederanno all'applicazione Web Security Agent (IAM Identity Center SSO o IAM-only accesso tramite la console AWS)
- Autorizzazioni: configura il ruolo IAM utilizzato dall'applicazione Web per accedere ai servizi AWS
- First Agent Space: crea il tuo Agent Space iniziale con un nome e una descrizione

> **Note**
>
> Dopo aver completato questa configurazione, creare Agent Spaces aggiuntivi è più semplice: basta fornire un nome e una descrizione. the section called "Crea uno spazio per agenti"Per ulteriori dettagli sulla creazione di Agent Spaces successivi, vedere.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Autorizzazioni per creare e gestire risorse AWS Security Agent
- Comprensione dei requisiti di gestione delle identità della tua organizzazione
- (Facoltativo) Account AWS con autorizzazioni per creare ruoli IAM e configurare IAM Identity Center (se si utilizza l'accesso SSO)
- (Facoltativo) Ruolo IAM esistente se desideri utilizzare una configurazione di autorizzazioni personalizzata

Fase 1: Crea il tuo primo Agent Space

Definite le proprietà di base del vostro primo Agent Space che verranno visualizzate agli utenti nell'applicazione web.

1. Nella pagina della console AWS Security Agent, scegli Configura Security Agent.
2. Nel campo Agent Space name, inserisci un nome per il tuo Agent Space.

> **Note**
>
> Il nome di Agent Space viene visualizzato agli utenti nell'applicazione Web e aiuta a identificare l'applicazione o il progetto rappresentato da questo spazio.

3. (Facoltativo) Nel campo Descrizione, fornite una descrizione che aiuti a distinguere lo scopo di Agent Space.

> **Tip**
>
> La descrizione aiuta a distinguere lo scopo di Agent Space. Ti consigliamo di descrivere l'applicazione o il progetto specifico che questo Agent Space proteggerà, ad esempio

«Applicazione web del portale clienti» o «Microservizi per l'elaborazione dei pagamenti» o «Piattaforma di analisi interna».

Passaggio 2: scegli il metodo di accesso

Seleziona in che modo gli utenti accederanno all'applicazione Web Security Agent. Puoi scegliere tra abilitare l'accesso SSO tramite IAM Identity Center o fornire l'accesso tramite la console AWS.

> **Note**
>
> Se scegli IAM-only l'accesso e successivamente desideri utilizzare IAM Identity Center, dovrai eliminare la configurazione di AWS Security Agent e completare nuovamente il processo di configurazione.

1. Nella sezione Metodo di accesso, seleziona una delle seguenti opzioni:
   - IAM Identity Center (SSO): abilita l'accesso SSO per il tuo team tramite IAM Identity Center. Questa opzione è consigliata per i team che necessitano di una gestione centralizzata degli utenti e desiderano che gli utenti accedano direttamente all'applicazione Web senza passare dalla Console AWS.
   - IAM-only accesso: fornisci l'accesso tramite un link di accesso da amministratore nella console AWS. Questa opzione è più semplice da configurare e adatta ai team che preferiscono l'accesso da console o che non richiedono funzionalità SSO.
2. Se hai selezionato IAM Identity Center (SSO), continua con la Fase 2a riportata di seguito.
3. Se hai selezionato IAM-only l'accesso, vai alla Fase 3.

Fase 2a: Configurazione di IAM Identity Center (solo accesso SSO)

Completa questi passaggi solo se hai selezionato IAM Identity Center (SSO) come metodo di accesso.

1. Nella sezione Connect to IAM Identity Center, esamina la regione AWS.

> **Important**
>
> La tua applicazione deve essere configurata nella stessa regione in cui abiliti IAM Identity Center. La regione visualizzata è quella in cui verrà creato il tuo Agent Space. IAM Identity Center deve essere abilitato nella stessa regione in cui crei l'Agent Space.

2. Nella sezione IAM Identity Center, scegli una delle seguenti opzioni:
   - Scegli Crea un'istanza di account per creare una nuova istanza di account IAM Identity Center
   - Se un'istanza dell'organizzazione esiste già nella stessa regione, AWS Security Agent si connetterà automaticamente ad essa

   > **Note**
   >
   > Dopo che AWS Security Agent è connesso a IAM Identity Center, puoi gestire l'accesso assegnando gli utenti in IAM Identity Center all'applicazione.

3. Se stai collegando Active Directory o un provider di identità esterno, esamina l'avviso informativo.

> **Important**
>
> Se gestisci già gli utenti in Active Directory o in un'altra fonte di identità e prevedi di connettere tale fonte di identità a IAM Identity Center, annulla la configurazione e vai prima alla console IAM Identity Center. Scegli la fonte di identità a cui desideri connettere prima di configurare AWS Security Agent. La modifica delle fonti di identità in un secondo momento potrebbe rimuovere le assegnazioni degli utenti esistenti.

Passaggio 3: Configurazione delle autorizzazioni (opzionale)

Configura il ruolo IAM utilizzato dalla tua applicazione Web Security Agent per accedere ai servizi, alle API e agli account AWS.

1. Individua la configurazione delle autorizzazioni, sezione opzionale.
2. Se la sezione è compressa, scegli la sezione Configurazione delle autorizzazioni per espanderla.
3. Seleziona una delle seguenti opzioni:

- Crea un ruolo predefinito: AWS Security Agent crea automaticamente un nuovo ruolo IAM con le autorizzazioni necessarie per l'applicazione Web
- Usa un altro ruolo: seleziona un ruolo IAM esistente tra le opzioni disponibili

4. Esamina la descrizione del ruolo:

> **Note**
>
> Verrà creato un ruolo IAM predefinito per l'applicazione Web per accedere ad altri servizi, API e account AWS. Al ruolo verranno concesse le autorizzazioni necessarie per le operazioni di valutazione della sicurezza.

Fase 4: Configurazione completa

Dopo aver configurato tutte le impostazioni richieste, completa la configurazione per creare il primo Agent Space e avviare l'applicazione Web Security Agent.

1. Rivedi tutte le sezioni di configurazione per garantire l'accuratezza.
2. Scegliere Set up (Configura).
3. AWS Security Agent crea il tuo Agent Space, stabilisce l'applicazione Web e configura le risorse AWS necessarie.

> **Note**
>
> Dopo la configurazione iniziale, avrai la possibilità di configurare funzionalità tra cui limiti dei test di penetrazione, requisiti di sicurezza e integrazione. GitHub

Fasi successive

Dopo aver configurato AWS Security Agent:

- Definisci i requisiti di sicurezza per la tua organizzazione
- Configura le funzionalità di test di penetrazione, tra cui la verifica del dominio e l'accesso VPC per il tuo Agent Space
- Connect GitHub repository per la revisione del codice e il contesto dei test di penetrazione

- (Se si utilizza IAM Identity Center) Assegna gli utenti all'Agent Space nella console AWS Security Agent
- (Se usi IAM-only access) Avvia l'applicazione Web tramite il link di accesso amministratore nella console AWS
- Crea Agent Spaces aggiuntivi per altre applicazioni (vedithe section called "Crea uno spazio per agenti")

Crea uno spazio per agenti

Crea Agent Spaces per proteggere applicazioni o progetti nella tua organizzazione. Ogni Agent Space offre uno spazio di lavoro per valutazioni, risultati e configurazioni di sicurezza specifici per quell'applicazione o progetto ed è accessibile da più utenti.

Questa procedura presuppone che tu abbia già completato la configurazione iniziale di AWS Security Agent. Se non hai ancora configurato AWS Security Agent, consultathe section called "Configurazione di AWS Security Agent".

Panoramica di

Comprendere Agent Spaces

Un Agent Space è uno spazio di lavoro dedicato per proteggere un'applicazione o un progetto specifico. Contiene tutte le revisioni di sicurezza, gli archivi di codice collegati opzionalmente, le configurazioni dei test di penetrazione, i risultati e i risultati per quell'applicazione.

Agent Spaces ti aiuta a organizzare il lavoro di sicurezza mantenendo separate le valutazioni di sicurezza di ciascuna applicazione, permettendo ai team di concentrarsi sulla propria applicazione specifica. Ti consigliamo di creare un Agent Space per applicazione o progetto per mantenere confini chiari.

Per una spiegazione completa di Agent Spaces e di come si inseriscono nella struttura di sicurezza dell'organizzazione, consultathe section called "Comprendi la gerarchia e il ciclo di vita delle risorse".

Cosa è incluso in un Agent Space

Ogni Agent Space contiene:

- Archivi di codice collegati opzionalmente associati all'applicazione o al progetto

- Revisioni progettuali precedenti dell'applicazione o del progetto
- Configurazioni e limiti dei test di penetrazione specifici dell'applicazione
- Risultati dei test di penetrazione e risultati di sicurezza

Crea uno spazio per agenti

Crea un nuovo Agent Space per un'applicazione o un progetto che desideri proteggere.

1. Nella console AWS Security Agent, vai alla pagina Agent Spaces.
2. Scegli Create Agent Space.
3. Nel campo Agent Space name, inserisci un nome per il tuo Agent Space.

> **Note**
>
> Il nome di Agent Space viene visualizzato agli utenti nell'applicazione Web e aiuta a identificare l'applicazione o il progetto rappresentato da questo spazio.

4. (Facoltativo) Nel campo Descrizione, fornite una descrizione che aiuti a distinguere lo scopo di Agent Space.

> **Tip**
>
> La descrizione aiuta a distinguere lo scopo di Agent Space. Ti consigliamo di descrivere l'applicazione o il progetto specifico che questo Agent Space proteggerà, ad esempio «Applicazione web del portale clienti» o «Microservizi per l'elaborazione dei pagamenti» o «Piattaforma di analisi interna».

5. Scegli Create (Crea).

> **Note**
>
> AWS Security Agent creerà il tuo Agent Space. Ora puoi configurare funzionalità e connettere risorse specifiche per questa applicazione.

Fasi successive

Dopo aver creato il tuo Agent Space:

- Connect i repository di codice sorgente (GitHub GitLab, Bitbucket o GitHub Enterprise Server) per la revisione del codice e il contesto dei test di penetrazione
- Connect Confluence per il contesto della documentazione nelle revisioni dei progetti e nei test di penetrazione
- Abilita la funzionalità di revisione del codice per i repository connessi (vedi) the section called "Abilita la revisione del codice pull request per i GitHub repository"
- Configura le funzionalità di penetration test, inclusa la verifica del dominio
- (Se utilizzi IAM Identity Center) Assegna gli utenti a questo Agent Space nella sezione Web App della pagina Agent Space. (vedithe section called "Concedi agli utenti l'accesso all'app Web AWS Security Agent")
- (Se si utilizza IAM-only l'accesso) Gli utenti con accesso alla console possono avviare l'applicazione Web tramite il collegamento di accesso amministrativo per questo Agent Space

Integrazioni Connect

Connect e gestisci i provider di codice sorgente (GitHub GitLab, Bitbucket ed GitHub Enterprise Server) e i fornitori di documentazione (Confluence), oltre alla connettività di rete privata, che i tuoi Agent Spaces utilizzano per la revisione del codice, i test di penetrazione e la modellazione delle minacce.

Come funzionano le integrazioni con Agent Spaces

AWS Security Agent si collega a fornitori di codice sorgente e documentazione di terze parti in modo che l'agente possa analizzare il codice e la documentazione durante le valutazioni di sicurezza. Prima di collegare un provider specifico, è utile capire in che modo le integrazioni si relazionano agli Agent Spaces e alle funzionalità.

Registrati una volta, riutilizza ovunque

La connessione di un provider ad AWS Security Agent prevede due passaggi distinti che avvengono a diversi livelli:

1. Registra l'integrazione (a livello di account). È possibile registrare un provider una sola volta dalla pagina Integrazioni nella Console di gestione di AWS Security Agent. Una registrazione rappresenta la connessione autorizzata a un account provider, ad esempio GitHub un'organizzazione, un GitLab gruppo, uno spazio di lavoro Bitbucket o un sito Confluence. Le registrazioni sono risorse a livello di account.

2. Connect le risorse a un Agent Space (livello Agent Space). Dall'interno di un Agent Space, connetti le risorse da un'integrazione registrata (repository per i fornitori di codice sorgente o pagine per Confluence) e configuri il modo in cui l'agente le utilizza. Questo passaggio è specifico per ogni Agent Space.

Una singola registrazione viene riutilizzata in ogni Agent Space del tuo account. Se hai registrato un provider durante la configurazione di un Agent Space, la stessa registrazione è disponibile quando colleghi le risorse a un altro Agent Space: non registri più lo stesso provider.

Una connessione, condivisa tra tutte le funzionalità

Quando connetti una risorsa a un Agent Space, tale risorsa viene condivisa tra le funzionalità dell'agente. Non si connette un repository separatamente per ogni funzionalità.

- L'accesso in lettura viene garantito collegando la risorsa. La connessione di un repository consente ad AWS Security Agent di leggerlo per scansioni complete del codice (revisione del codice), contesto dei test di penetrazione, modellazione delle minacce e revisione del progetto. Il collegamento di una pagina Confluence consente all'agente di leggerla per il contesto della documentazione relativa alle revisioni di progettazione, alla modellazione delle minacce e ai test di penetrazione.
- Le azioni di scrittura sono facoltative, a seconda del repository. Quando connetti i repository di codice sorgente a un Agent Space, puoi inoltre abilitare le azioni di scrittura per ogni repository:
  - Commenti sulla revisione del codice: AWS Security Agent pubblica i risultati della revisione sotto forma di commenti su richieste pull (o richieste di unione GitLab).
  - Correzione del codice: AWS Security Agent apre le richieste pull (o merge request) con correzioni per le vulnerabilità scoperte.

    Queste azioni di scrittura non sono disponibili per gli archivi pubblici. Read-only l'analisi è ancora valida.

> **Note**
>
> Confluence è un fornitore di documentazione piuttosto che un fornitore di codice sorgente. AWS Security Agent legge le pagine connesse di Confluence per fornire un contesto per le revisioni di progettazione, la modellazione delle minacce e i test di penetrazione. La selezione

di una pagina consente l'accesso in lettura; non sono previsti interruttori di funzionalità per pagina.

Provider supportati

AWS Security Agent supporta i seguenti provider:

- Codice sorgente: GitHub (Enterprise ospitato nel cloud GitHub e nel cloud), GitHub GitHub Enterprise Server (ospitato autonomamente), (ospitato nel cloud), GitLab (ospitato autonomamente) e Bitbucket GitLab Self-Managed Cloud.
- Documentazione - Confluence Cloud.

Per i provider con hosting autonomo che non sono raggiungibili sulla rete Internet pubblica, puoi indirizzare il traffico dell'agente tramite una connessione privata. Per ulteriori informazioni, consulta the section called “Connect al controllo del codice sorgente ospitato privatamente”.

Fasi successive

- Registra un provider dalla pagina Integrazioni. Consulta l'argomento relativo alla connessione per il tuo provider, ad esempiothe section called “Connect AWS Security Agent ai GitHub repository”.
- Connect le risorse a un Agent Space e configura le funzionalità. Consulta the section called “Abilita la revisione del codice” e the section called “Abilita il test di penetrazione”.

Connect AWS Security Agent ai GitHub repository

Connect AWS Security Agent ai GitHub repository per abilitare funzionalità di revisione del codice, modellazione delle minacce, penetration test e correzione automatica. AWS Security Agent supporta sia le aziende ospitate nel cloud che quelle ospitate GitHub nel cloud GitHub . Prima di iniziare, esamina the section called “Come funzionano le integrazioni con Agent Spaces” per capire come una registrazione viene riutilizzata tra Agent Spaces e condivisa tra le funzionalità.

GitHub l'integrazione serve a molteplici scopi:

> **Note**
>
> Questa pagina riguarda Enterprise ospitata nel cloud GitHub (github.com) e ospitata nel cloud. GitHub Per Enterprise Server con hosting autonomo, vedere. GitHub the section called "Connect AWS Security Agent a GitHub Enterprise Server"

- Revisione del codice: analizza automaticamente le modifiche al codice in ogni pull request rispetto ai requisiti di sicurezza dell'organizzazione ed esegui scansioni complete dell'archivio su richiesta
- Modellazione delle minacce: consente di comprendere le applicazioni analizzando il codice sorgente, i flussi di dati e l'architettura
- Contesto dei test di penetrazione: consente di comprendere le applicazioni per i test di penetrazione analizzando il codice sorgente
- Correzione automatizzata: invia richieste pull con correzioni per le vulnerabilità scoperte durante le valutazioni di sicurezza

La connessione GitHub ad AWS Security Agent richiede l'autorizzazione dell' GitHub app AWS Security Agent per l' GitHub organizzazione o l'account utente, quindi la registrazione della connessione nella Console AWS.

Come funziona GitHub l'integrazione

L'analisi delle pull request avviene all'interno GitHub. Dopo aver autorizzato l' GitHub app, collegato gli repository e abilitato i commenti di revisione del codice nella Console di gestione AWS, AWS Security Agent analizza automaticamente le modifiche in ogni nuova pull request (una scansione differenziale del solo codice modificato) e pubblica i risultati come commenti di pull request.

Puoi creare ed eseguire revisioni complete del codice, che scansionano l'intera base di codice di un repository, nell'applicazione Web AWS Security Agent, non in. GitHub

I test di penetrazione e la modellazione delle minacce vengono avviati all'interno dell'applicazione Web AWS Security Agent. Gli utenti selezionano i repository connessi per fornire il contesto dell'applicazione e specificano i domini di destinazione per i test di penetrazione. Se abiliti la correzione automatica, gli utenti possono richiedere ad AWS Security Agent di correggere i risultati aprendo richieste pull ai repository collegati.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- GitHub accesso all'amministratore dell'organizzazione o accesso al proprietario GitHub dell'account utente
- Autorizzazioni per configurare le integrazioni per il tuo Agent Space nella Console di gestione AWS
- Comprensione dei repository da collegare per la revisione del codice, la modellazione delle minacce e i test di penetrazione

Important

Un' GitHub app può essere installata solo una volta su un GitHub account o un'organizzazione. GitHub Se devi connettere la stessa GitHub organizzazione ad AWS Security Agent, devi utilizzare lo stesso account AWS in cui l'integrazione è stata registrata per la prima volta.

Note

Se la tua organizzazione GitHub aziendale ha abilitato l'elenco degli indirizzi IP consentiti, devi accettare gli indirizzi IP consentiti sull' GitHub app. Puoi anche scegliere di aggiungere automaticamente gli indirizzi IP all'elenco degli elementi consentiti. Per ulteriori informazioni, consulta Consentire l'accesso da parte GitHub delle app e Abilitare gli indirizzi IP consentiti nella GitHub documentazione.
I seguenti indirizzi IP vengono utilizzati per accedere alle GitHub risorse:

- Stati Uniti orientali (Virginia settentrionale) (us-east-1)
  - `34.228.181.128`
  - `44.219.176.187`
  - `54.226.244.221`
- Stati Uniti occidentali (Oregon) (us-west-2)
  - `34.212.16.133`
  - `52.89.67.212`
  - `54.187.135.61`

- Asia Pacifico (Mumbai) (ap-south-1)
  - `13.126.209.199`
  - `13.234.6.24`
  - `35.154.102.216`
- Asia Pacifico (Singapore) (ap-southeast-1)
  - `18.139.13.125`
  - `47.130.240.215`
  - `54.179.238.173`
- Asia Pacifico (Sydney) (ap-southeast-2)
  - `13.237.95.197`
  - `13.238.84.102`
  - `52.64.174.242`
- Asia Pacifico (Tokyo) (ap-northeast-1)
  - `13.192.12.233`
  - `35.74.181.230`
  - `57.183.50.158`
- Europa (Francoforte) (eu-central-1)
  - `18.158.110.140`
  - `52.57.96.160`
  - `52.59.55.56`
- Europa (Irlanda) (eu-west-1)
  - `34.251.85.24`
  - `52.30.157.157`
  - `52.51.192.222`
- Sud America (San Paolo) (sa-east-1)
  - `54.94.247.213`
  - `54.207.222.14`
  - `54.232.201.242`

Autorizza e registra l'app AWS Security Agent GitHub

Autorizza l' GitHub app AWS Security Agent ad accedere alla tua GitHub organizzazione o al tuo account utente, quindi registra la connessione nella Console AWS.

> **Important**
>
> Completa tutti i passaggi di questo processo senza chiudere il browser o allontanarti. Se il processo di registrazione viene interrotto, potrebbe essere necessario disinstallare l' GitHub app e ricominciare da capo.

1. Nella Console di gestione di AWS Security Agent, vai a Integrazioni.
2. Scegli Aggiungi integrazione.
3. Seleziona GitHub.
4. Scegli Next (Successivo).
5. Scegli Installa e autorizza.

   Verrai reindirizzato a GitHub completare l'autorizzazione. Assicurati di aver effettuato l'accesso GitHub con un account con accesso amministrativo all'organizzazione o all'account utente a cui desideri connettere.
6. In GitHub, seleziona l'account o l'organizzazione in cui desideri installare l' GitHub app AWS Security Agent.
7. Seleziona a quali repository può accedere AWS Security Agent:
   - Tutti gli archivi: concedi l'accesso a tutti gli archivi attuali e futuri dell'organizzazione o dell'account utente
   - Seleziona solo i repository: scegli i repository specifici dal menu a discesa. Puoi selezionare più repository uno alla volta.

   > **Note**
   >
   > Puoi modificare l'accesso al repository in qualsiasi momento visitando le impostazioni dell' GitHub app nella tua GitHub organizzazione o nelle impostazioni dell'account utente.
8. Scegli Installa e autorizza.

9. Verrai reindirizzato alla Console di gestione AWS per completare la registrazione.
10. Nella sezione Dettagli di registrazione, configura i seguenti campi:
    a. Nome di registrazione: inserisci un nome descrittivo per questa GitHub connessione. Utilizza un nome che identifichi l' GitHub organizzazione o l'account utente, ad esempio "" o Acme-Corp-Org "»Production-Repos.
    b. Tipo di account: seleziona una delle seguenti opzioni dal menu a discesa:
        - Organizzazione: se hai collegato un account GitHub aziendale
        - Utente: se hai collegato un account GitHub utente personale
    c. Nome dell'organizzazione (appare solo se hai selezionato Organizzazione): inserisci il nome esatto GitHub dell'organizzazione così come appare in GitHub.
11. Scegli Connetti.
12. Viene visualizzato un messaggio di conferma e si torna alla pagina Integrazioni, dove viene visualizzata la nuova GitHub connessione con il nome di registrazione. Per connettere altre GitHub organizzazioni o account utente, ripeti questa procedura selezionando nuovamente Aggiungi integrazione.

Risolvi i problemi GitHub di integrazione

Se riscontri problemi durante il processo di GitHub integrazione, utilizza la seguente guida per risolvere i problemi più comuni.

Impossibile completare la registrazione

Se non sei riuscito a completare il processo di registrazione (ad esempio, il browser è stato chiuso, ti sei allontanato dalla pagina di registrazione o hai riscontrato un'interruzione della sessione), GitHub l'app AWS Security Agent potrebbe essere installata nell' GitHub organizzazione ma non registrata nella Console AWS.

Caratteristiche:

- Quando tenti di autorizzare nuovamente l' GitHub app, GitHub mostra «Configura» anziché «Installa»
- Non è possibile completare la registrazione nella console AWS
- L'integrazione non viene visualizzata nell'elenco delle integrazioni

Risoluzione:

1. Disinstalla l' GitHub app AWS Security Agent dalla tua GitHub organizzazione o dal tuo account utente.
2. Torna alla console AWS Security Agent e riavvia il processo di integrazione dall'inizio.

Più account AWS che cercano di integrare la stessa GitHub organizzazione

Un' GitHub app può essere installata una sola volta su un GitHub account o GitHub un'organizzazione. Se è necessario utilizzare repository di GitHub un'organizzazione già integrata con un altro account AWS Security Agent, è necessario utilizzare l'account AWS in cui l'integrazione è stata registrata per la prima volta.

Risoluzione:

- Identifica in quale account AWS Security Agent è registrata l' GitHub integrazione
- Usa quell'account AWS per creare Agent Spaces e connettere repository
- Se devi spostare l'integrazione su un altro account AWS, disinstalla prima l' GitHub app dall'account AWS originale, quindi integrala con il nuovo account

Fasi successive

Dopo la connessione GitHub ad AWS Security Agent:

- Accedi all'Agent Space in cui desideri utilizzare questi repository
- Scegli Enable code review o Setup penetration testing per connettere repository specifici a Agent Space e configurarne l'utilizzo
- Abilita la correzione automatica per consentire ad AWS Security Agent di inviare richieste pull con correzioni di vulnerabilità
- Controlla le autorizzazioni GitHub dell'app e l'accesso al repository nelle impostazioni della tua organizzazione GitHub

Rimuovere un' GitHub integrazione

Rimuovi un' GitHub integrazione quando non hai più bisogno di AWS Security Agent per accedere ai repository da un' GitHub organizzazione o un account utente specifici. Devi prima disinstallare l' GitHub app AWS Security Agent GitHub prima di rimuovere l'integrazione nella Console AWS.

Prerequisiti per la rimozione

Prima di rimuovere un' GitHub integrazione, assicurati di avere:

- Hai verificato quali Agent Spaces dispongono di repository collegati da questa integrazione
- Compreso l'impatto: la rimozione di questa integrazione interromperà le connessioni ai repository per la revisione del codice, il contesto dei test di penetrazione e la correzione dei test di penetrazione in tutti gli Agent Spaces che utilizzano i repository di questa integrazione
- GitHub accesso all'amministratore dell'organizzazione o accesso al proprietario dell'account utente per disinstallare l'app GitHub

Fase 1: Disinstalla l' GitHub app AWS Security Agent da GitHub

Innanzitutto, disinstalla l' GitHub app AWS Security Agent dalla tua GitHub organizzazione o dall'account utente.

Per GitHub le organizzazioni:

1. Vai su github.com e apri la pagina della tua organizzazione.
2. Nella barra laterale sinistra, scegli Impostazioni.
3. In Codice, pianificazione e automazione, scegli GitHub App installate.
4. Individua l'app AWS Security Agent nell'elenco.
5. Scegli Configure accanto all'app AWS Security Agent.
6. Scorri fino alla fine della pagina di configurazione e scegli Disinstalla.
7. Conferma la disinstallazione quando richiesto.

Per gli account GitHub utente:

1. Vai su github.com.
2. Scegli la tua immagine del profilo.
3. Seleziona Impostazioni.
4. Nella barra laterale sinistra, seleziona Applicazioni.
5. Apri la scheda GitHub App installate.
6. Individua l'app AWS Security Agent nell'elenco.
7. Scegli Configure accanto all'app AWS Security Agent.

8. Scorri fino alla fine della pagina di configurazione e scegli Disinstalla.
9. Conferma la disinstallazione quando richiesto.

Fase 2: rimuovere l'integrazione da AWS Security Agent

Dopo aver disinstallato l' GitHub app, rimuovi la registrazione dell'integrazione dalla console AWS.

1. Nella Console di gestione di AWS Security Agent, vai a Integrazioni.
2. Individua l' GitHub integrazione che desideri rimuovere nell'elenco delle integrazioni.
3. Seleziona l'integrazione facendo clic su di essa.
4. Scegli Rimuovi.
5. Esamina la finestra di dialogo di conferma, che ti avvisa dell'impatto:

> **Warning**
>
> La rimozione di questa integrazione avrà effetto su tutti gli Agent Spaces che dispongono di repository collegati da questa GitHub organizzazione o account utente. Ciò interromperà:
>
> - Funzionalità di revisione del codice per gli archivi connessi
> - Contesto di test di penetrazione da repository collegati
> - Funzionalità di correzione dei test di penetrazione per gli archivi connessi
>
> Assicurati di aver disinstallato l' GitHub app AWS Security Agent GitHub prima di procedere.

6. Se non hai ancora disinstallato l' GitHub app da GitHub, riceverai un avviso. Torna al passaggio 1 per completare prima la disinstallazione.
7. Se hai disinstallato l' GitHub app e ne comprendi l'impatto, scegli Conferma rimozione.
8. L'integrazione viene rimossa dall'elenco delle integrazioni. Qualsiasi Agent Spaces con i repository di questa integrazione non ha più accesso a tali repository per la revisione del codice, il contesto dei test di penetrazione o la correzione automatica.

Connect AWS Security Agent ai GitLab repository

Connetti il tuo AWS Security Agent ai repository GitLab cloud per abilitare funzionalità di revisione del codice, modellazione delle minacce, test di penetrazione e correzione automatizzata. Prima di

iniziare, esamina the section called "Come funzionano le integrazioni con Agent Spaces" per capire come una registrazione viene riutilizzata tra Agent Spaces e condivisa tra le funzionalità.

GitLab l'integrazione serve a molteplici scopi:

- Revisione del codice: analizza automaticamente le modifiche al codice in ogni richiesta di unione rispetto ai requisiti di sicurezza dell'organizzazione ed esegui scansioni complete dell'archivio su richiesta
- Modellazione delle minacce: consente di comprendere le applicazioni analizzando il codice sorgente, i flussi di dati e l'architettura
- Contesto dei test di penetrazione: consente di comprendere le applicazioni per i test di penetrazione analizzando il codice sorgente
- Correzione automatizzata: invia richieste di unione con correzioni per le vulnerabilità scoperte durante le valutazioni di sicurezza

La connessione GitLab ad AWS Security Agent richiede la fornitura di un token di GitLab accesso con le autorizzazioni appropriate, quindi la registrazione della connessione nella Console AWS.

Come funziona GitLab l'integrazione

L'analisi delle richieste di unione avviene all'interno GitLab. Dopo aver fornito il token di accesso, collegato i progetti e abilitato i commenti di revisione del codice nella Console di gestione AWS, AWS Security Agent analizza automaticamente le modifiche in ogni nuova richiesta di unione (una scansione differenziale del solo codice modificato) e pubblica i risultati come commenti alla richiesta di unione.

Puoi creare ed eseguire revisioni complete del codice, che scansionano l'intera base di codice di un progetto, nell'applicazione Web AWS Security Agent, non in GitLab.

I test di penetrazione e la modellazione delle minacce vengono avviati all'interno dell'applicazione Web AWS Security Agent. Gli utenti specificano i domini di destinazione e selezionano i repository connessi per fornire il contesto dell'applicazione. Se abiliti la correzione automatica, gli utenti possono richiedere ad AWS Security Agent di correggere i risultati aprendo richieste di unione ai repository collegati.

> **Note**
>
> La riparazione automatica non è disponibile per gli GitLab archivi pubblici per evitare di rivelare le vulnerabilità prima che vengano corrette.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Un GitLab.com account con accesso da Maintainer o Owner ai progetti che desideri connettere
- Un token di GitLab accesso con gli ambiti necessari per il tipo di connessione:
  - Personale: un token di accesso personale con tutte le autorizzazioni di lettura e l'`api`autorizzazione.
  - Gruppo: un token di accesso di gruppo con `read_repository` ambiti `read_api` e.
- Autorizzazioni per configurare le integrazioni nella console di gestione di AWS Security Agent

> **Important**
>
> Imposta la scadenza del token su un massimo di 365 giorni dopo la data corrente.

> **Note**
>
> GitLab I token di accesso personali possono essere utilizzati su più account AWS. A differenza delle GitHub integrazioni Atlassian, non ci sono restrizioni sulla connessione dello stesso account GitLab a più istanze di AWS Security Agent.

GitLab Registra una connessione

1. Nella Console di gestione di AWS Security Agent, vai a Integrazioni.
2. Scegli Aggiungi integrazione.
3. Seleziona GitLab, quindi scegli Avanti.
4. In Scegli un tipo di account, seleziona una delle seguenti opzioni:

- Personale: collega il tuo account GitLab utente individuale.
- Gruppo: collega un GitLab gruppo che contiene più progetti. Inserisci l'ID del tuo gruppo.

5. Nel campo Token di accesso, incolla il tuo token di GitLab accesso.
6. Nel campo Nome di registrazione, inserisci un nome descrittivo per questa connessione, ad esempio`Engineering-Team-GitLab`. I caratteri validi sono lettere, numeri, punti, caratteri di sottolineatura e trattini.
7. Scegli Connetti.

   Si torna alla pagina Integrazioni, dove viene visualizzata la nuova connessione con il nome di registrazione.

Risolvi i problemi GitLab di integrazione

Se riscontri problemi durante il processo di GitLab integrazione, utilizza la seguente guida per risolvere i problemi più comuni.

Token non valido o scaduto

Caratteristiche

- L'integrazione non riesce a connettersi
- L'integrazione precedentemente funzionante smette di funzionare
- Messaggio di errore che indica un errore di autenticazione

Risoluzione

1. In GitLab, accedi alle impostazioni utente e seleziona Access Tokens.
2. Verifica che il token non sia scaduto.
3. Verifica che il token abbia gli ambiti richiesti per il suo tipo.
4. Se il token è scaduto, crea un nuovo token e aggiorna l'integrazione nella console AWS.

Limitazione della velocità

Caratteristiche

- Guasti intermittenti durante la revisione del codice

- Analisi ritardata delle richieste di unione

Risoluzione

- GitLab applica limiti di velocità alle richieste API. Se disponi di un numero elevato di repository o di richieste di unione frequenti, alcune richieste potrebbero essere limitate.
- Attendi che la finestra del limite di velocità venga ripristinata o contatta l' GitLab assistenza per aumentare i limiti di velocità.

Fasi successive

Dopo la connessione GitLab ad AWS Security Agent:

- Accedi all'Agent Space in cui desideri utilizzare questi repository
- Scegli Enable code review o Setup penetration testing per connettere progetti specifici a Agent Space e configurarne l'utilizzo
- Abilita la correzione del codice per consentire ad AWS Security Agent di inviare richieste di unione con correzioni di vulnerabilità
- Per le istanze ospitate privatamente, vedi GitLab the section called "Connect AWS Security Agent a GitLab Self-Managed"

Connect AWS Security Agent a GitLab Self-Managed

Connetti il tuo AWS Security Agent a un' GitLab Self-Managed istanza per abilitare funzionalità di revisione del codice, modellazione delle minacce, test di penetrazione e riparazione automatizzata per i repository ospitati sulla tua infrastruttura.

GitLab Self-Managed l'integrazione funziona come nel GitLab cloud (vedithe section called "Connect AWS Security Agent ai GitLab repository") con una configurazione aggiuntiva per la connettività di rete alla tua istanza privata. Prima di iniziare, esamina the section called "Come funzionano le integrazioni con Agent Spaces" per capire come una registrazione viene riutilizzata in Agent Spaces e condivisa tra le funzionalità.

> **Note**
>
> GitLab Self-Managed viene registrata tramite l'GitLabintegrazione, non tramite un tipo di integrazione separato. Nel flusso di registrazione, selezioni Usa endpoint GitLab ospitato

autonomamente e fornisci l'URL dell'istanza. Il GitLab flusso ospitato nel cloud è descritto in. the section called "Connect AWS Security Agent ai GitLab repository"

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Un' GitLab Self-Managed istanza che è una delle seguenti:
  - Accessibile al pubblico tramite Internet, OPPURE
  - Accessibile tramite una connessione privata (vedithe section called "Connect al controllo del codice sorgente ospitato privatamente")
- Un token di GitLab accesso con gli ambiti richiesti per il tipo di connessione:
  - Personale: un token di accesso personale con tutte le autorizzazioni di lettura e l'`api`autorizzazione.
  - Gruppo: un token di accesso di gruppo con `read_repository` ambiti `read_api` e.
- Accesso da parte del manutentore o del proprietario ai progetti che desideri connettere
- L' GitLab istanza deve servire il traffico HTTPS con una versione TLS minima di 1.2

> **Note**
>
> Se l' GitLab Self-Managed istanza utilizza certificati TLS emessi da un'autorità di certificazione privata, puoi fornire la chiave PEM-encoded pubblica del certificato durante la creazione di una connessione privata. Ciò consente ad AWS Security Agent di affidare la connessione TLS alla tua istanza.

Registra una connessione GitLab Self-Managed

1. Nella Console di gestione di AWS Security Agent, vai a Integrazioni.
2. Scegli Aggiungi integrazione.
3. Seleziona GitLab, quindi scegli Avanti.
4. In Scegli un tipo di account, seleziona Personale o Gruppo. Se selezioni Gruppo, inserisci l'ID del gruppo.
5. Seleziona Usa endpoint GitLab ospitato autonomamente.

6. Nel campo URL dell'endpoint GitLab ospitato autonomamente, inserisci ad esempio l'URL della tua istanza. `https://gitlab.example.com`
7. Se la tua istanza non è accessibile pubblicamente, seleziona Connetti all'endpoint utilizzando una connessione privata, quindi scegli una connessione privata esistente o creane una nuova. Per informazioni, consulta the section called “Connect al controllo del codice sorgente ospitato privatamente”.
8. Nel campo Token di accesso, incolla il tuo token di GitLab accesso.
9. Nel campo Nome di registrazione, inserisci un nome descrittivo per questa connessione. I caratteri validi sono lettere, numeri, punti, caratteri di sottolineatura e trattini.
10. Scegli Connetti.

    Si torna alla pagina Integrazioni, dove viene visualizzata la nuova connessione con il nome di registrazione.

Connettività privata

Se la tua GitLab Self-Managed istanza non è accessibile al pubblico, devi creare una connessione privata prima di registrare l'integrazione. Vedi the section called “Connect al controllo del codice sorgente ospitato privatamente” per istruzioni dettagliate.

> **Important**
>
> Service-managed le connessioni private richiedono che l' GitLab Self-Managed istanza sia in esecuzione nello stesso account AWS in cui viene creato l'Agent Space. Per l'accesso a più account, utilizza una connessione privata autogestita in cui fornisci la tua configurazione delle risorse VPC Lattice.

Risolvi i problemi di integrazione GitLab Self-Managed

Oltre alla procedura di risoluzione dei problemi illustrata di seguitothe section called “Connect AWS Security Agent ai GitLab repository”, i seguenti problemi sono specifici delle istanze autogestite:

Istanza irraggiungibile

Caratteristiche

- La connessione fallisce a causa di un timeout o di un errore di rete

- L'integrazione funzionava in precedenza ma smette di funzionare

Risoluzione

- Verifica che l' GitLab istanza sia in esecuzione e accessibile
- Se utilizzi una connessione privata, verifica che il gateway di risorse VPC Lattice sia integro e che gli ENI dispongano di connettività di rete alla tua istanza
- Verifica che i gruppi di sicurezza consentano il traffico sulla porta configurata
- Verifica che il certificato TLS sia valido e non scaduto

Errori del certificato TLS

Caratteristiche

- La connessione fallisce con un SSL/TLS errore

Risoluzione

- Verifica che l'istanza utilizzi HTTPS con TLS 1.2 o versioni successive
- Se utilizzi un'autorità di certificazione privata, assicurati che la chiave PEM-encoded pubblica sia stata fornita durante la configurazione della connessione privata
- Verifica che il certificato non sia scaduto

Fasi successive

Dopo la connessione GitLab Self-Managed ad AWS Security Agent:

- Accedi all'Agent Space in cui desideri utilizzare questi repository
- Scegli Enable code review o Setup penetration testing per collegare progetti specifici
- Abilita la correzione del codice per le correzioni basate su richieste di unione

Rimuovere un' GitLab integrazione

Rimuovi un' GitLab integrazione quando non hai più bisogno di AWS Security Agent per accedere ai repository da un GitLab account o un gruppo specifico.

Prerequisiti per la rimozione

Prima di rimuovere un' GitLab integrazione, assicurati di avere:

- Hai verificato quali Agent Spaces hanno repository collegati da questa integrazione
- Compreso l'impatto: la rimozione di questa integrazione interromperà le connessioni ai repository per la revisione del codice, il contesto dei test di penetrazione, la modellazione delle minacce e la riparazione automatica in tutti gli Agent Spaces che utilizzano i repository di questa integrazione

Rimuovi l'integrazione da AWS Security Agent

1. Nella Console di gestione di AWS Security Agent, vai a Integrazioni.
2. Individua l' GitLab integrazione che desideri rimuovere.
3. Seleziona l'integrazione facendo clic su di essa.
4. Scegli Rimuovi.
5. Controlla la finestra di dialogo di conferma e scegli Conferma rimozione.

> **Note**
>
> Dopo aver rimosso l'integrazione, potresti anche voler revocare il token di accesso personale GitLab per impedire ulteriori accessi. Accedi alle impostazioni GitLab utente ed elimina o revoca il token.

Lo stesso processo si applica alle integrazioni. GitLab Self-Managed

Connect AWS Security Agent a GitHub Enterprise Server

Collega il tuo AWS Security Agent a un'istanza GitHub Enterprise Server (GHES) per abilitare la revisione del codice, la modellazione delle minacce, i test di penetrazione e le funzionalità di riparazione automatizzata per i repository ospitati sulla tua infrastruttura.

GitHub L'integrazione con Enterprise Server offre le stesse funzionalità di quelle ospitate nel cloud GitHub (vedi Connect AWS Security Agent ai GitHub repository) con una configurazione aggiuntiva per la connettività di rete alla tua istanza ospitata autonomamente. Prima di iniziare, esamina the section called "Come funzionano le integrazioni con Agent Spaces" per capire come una registrazione viene riutilizzata tra Agent Spaces e condivisa tra le funzionalità.

> **Note**
>
> GitHub Enterprise Server viene registrato tramite l'GitHubintegrazione, non tramite un tipo di integrazione separato. Nel flusso di registrazione scegli GitHub Enterprise Server come tipo di istanza. Il GitHub.com flusso ospitato nel cloud è descritto in. the section called "Connect AWS Security Agent ai GitHub repository"

Come funziona l'integrazione con GitHub Enterprise Server

L'analisi delle pull request avviene all'interno di GitHub Enterprise Server. Dopo aver autorizzato la connessione, collegato gli repository e abilitato i commenti di revisione del codice nella Console di gestione AWS, AWS Security Agent analizza automaticamente le modifiche in ogni nuova pull request (una scansione differenziale del solo codice modificato) e pubblica i risultati come commenti di pull request.

Puoi creare ed eseguire revisioni complete del codice, che scansionano l'intera base di codice di un repository, nell'applicazione Web AWS Security Agent, non in GitHub Enterprise Server.

I test di penetrazione e la modellazione delle minacce vengono avviati all'interno dell'applicazione Web AWS Security Agent. Gli utenti specificano i domini di destinazione e selezionano i repository connessi per fornire il contesto dell'applicazione. Se abiliti la correzione automatica, gli utenti possono richiedere ad AWS Security Agent di correggere i risultati aprendo richieste pull ai repository collegati.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Un'istanza di GitHub Enterprise Server che sia:
  - Accessibile pubblicamente tramite Internet, OPPURE
  - Accessibile tramite una connessione privata (vedithe section called "Connect al controllo del codice sorgente ospitato privatamente")
- Accesso da amministratore del sito o amministratore dell'organizzazione sull'istanza GHES
- L'istanza GHES deve servire il traffico HTTPS con una versione TLS minima di 1.2
- Autorizzazioni per configurare le integrazioni nella console di gestione di AWS Security Agent

> **Note**
>
> GitHub Le integrazioni di Enterprise Server possono essere utilizzate su più account AWS.

Registra una connessione GitHub Enterprise Server

La registrazione di una connessione GitHub Enterprise Server utilizza un flusso di OAuth-based autorizzazione.

> **Important**
>
> Completa tutti i passaggi di questo processo senza chiudere il browser o allontanarsi. Se il processo di registrazione viene interrotto, potrebbe essere necessario riavviarlo dall'inizio.

1. Nella Console di gestione di AWS Security Agent, vai a Integrazioni.
2. Scegli Aggiungi integrazione.
3. Seleziona GitHub, quindi scegli Avanti.
4. In Tipo di istanza, seleziona GitHub Enterprise Server.
5. Nel campo URL GitHub Enterprise Server, inserisci l'URL HTTPS dell'istanza, ad esempio`https://github.example.com`.
6. Se la tua istanza non è accessibile pubblicamente, seleziona Connetti all'endpoint utilizzando una connessione privata, quindi scegli una connessione privata esistente o creane una nuova. Per informazioni, consulta the section called “Connect al controllo del codice sorgente ospitato privatamente”.
7. Nella sezione Dettagli del registro, configura i seguenti campi:
   a. Nome di registrazione: inserisci un nome descrittivo per questa connessione. I caratteri validi sono lettere, numeri, punti, caratteri di sottolineatura e trattini.
   b. GitHub tipo di account: seleziona Organizzazione o Utente.
   c. Nome dell'organizzazione (viene visualizzato solo se è stata selezionata l'opzione Organizzazione): immettere il nome esatto dell'organizzazione GitHub Enterprise Server. I nomi rispettano la distinzione tra lettere maiuscole e minuscole.
8. Scegli Connetti.

> **Note**
>
> AWS Security Agent ti reindirizza lontano dalla console per completare l'autorizzazione con la tua istanza GitHub Enterprise Server. Una volta completata l'autorizzazione, torni alla console e la nuova connessione viene visualizzata nella pagina Integrazioni.

Connettività privata

Se l'istanza di GitHub Enterprise Server non è accessibile pubblicamente, è necessario creare una connessione privata prima di registrare l'integrazione. the section called "Connect al controllo del codice sorgente ospitato privatamente"Per istruzioni dettagliate, vedere.

> **Important**
>
> Service-managed le connessioni private richiedono che l'istanza GHES sia in esecuzione nello stesso account AWS in cui viene creato l'Agent Space. Per l'accesso a più account, utilizza una connessione privata autogestita.

> **Note**
>
> Se la tua istanza GHES utilizza certificati TLS emessi da un'autorità di certificazione privata, fornisci la chiave PEM-encoded pubblica del certificato durante la creazione della connessione privata.

Risolvi i problemi GitHub di integrazione con Enterprise Server

Se riscontri problemi di connessione di AWS Security Agent a GitHub Enterprise Server, utilizza le seguenti linee guida per diagnosticare e risolvere i problemi più comuni.

Errore di reindirizzamento OAuth

Caratteristiche

- I reindirizzamenti del browser non riescono durante il flusso di autorizzazione
- Pagina di errore visualizzata dopo l'autorizzazione su GHES

Risoluzione

- Verifica che la tua istanza GHES sia accessibile dal tuo browser
- Assicurati che l'URL di callback OAuth sia configurato correttamente
- Riavvia il processo di integrazione dall'inizio

Istanza irraggiungibile

Caratteristiche

- La connessione fallisce a causa di un timeout o di un errore di rete

Risoluzione

- Verifica che l'istanza GHES sia in esecuzione e accessibile
- Se utilizzi una connessione privata, verifica la connettività VPC Lattice
- Verifica che i gruppi di sicurezza consentano il traffico sulla porta configurata
- Verifica che il certificato TLS sia valido (minimo TLS 1.2)

Fasi successive

Dopo aver collegato GitHub Enterprise Server ad AWS Security Agent:

- Accedi all'Agent Space in cui desideri utilizzare questi repository
- Scegli Enable code review o Setup penetration testing per connettere repository specifici
- Abilita la correzione del codice per consentire ad AWS Security Agent di inviare richieste pull con correzioni di vulnerabilità

Rimuovere un'integrazione con GitHub Enterprise Server

Rimuovi un'integrazione con GitHub Enterprise Server quando non hai più bisogno di AWS Security Agent per accedere ai repository da un'istanza GHES specifica.

Prerequisiti per la rimozione

Prima di rimuovere un'integrazione GHES:

- Verifica a quali Agent Spaces sono collegati i repository da questa integrazione
- Comprendi l'impatto: la rimozione interromperà la revisione del codice, il contesto dei test di penetrazione, la modellazione delle minacce e la correzione automatica per tutti gli archivi connessi

Rimuovi l'integrazione

1. Nella Console di gestione di AWS Security Agent, vai a Integrazioni.
2. Individua l'integrazione GitHub Enterprise Server che desideri rimuovere.
3. Seleziona l'integrazione.
4. Scegli Rimuovi.
5. Rivedi la finestra di dialogo di conferma e scegli Conferma rimozione.

> **Note**
>
> Dopo la rimozione, potresti anche voler revocare l'applicazione OAuth sulla tua istanza GHES. Accedi alle impostazioni dell'organizzazione GHES e rimuovi l'applicazione autorizzata.

Trova il tuo ID di installazione Atlassian

Prima di registrare un'integrazione di Bitbucket o Confluence nella console AWS, devi trovare l'ID di installazione dall'app AWS Security Agent Forge installata sul tuo sito Atlassian. Incolla questo ID nel flusso di registrazione.

Per Bitbucket

1. In Bitbucket, accedi alle impostazioni del tuo Workspace.
2. Seleziona Forge Apps dalla barra laterale.
3. Individua Connect with AWS Security Agent nell'elenco delle app installate.
4. Scegli Copia negli Appunti per copiare l'ID di installazione.

Per Confluence

1. In Confluence, accedi all'amministrazione di Confluence.

2. Seleziona App dalla barra laterale.
3. Individua Connect with AWS Security Agent nell'elenco delle app installate.
4. Scegli Copia negli Appunti per copiare l'ID di installazione.

Avrai bisogno di questo ID di installazione per completare la registrazione nella Console di gestione di AWS Security Agent.

Connect AWS Security Agent ai repository Bitbucket

Connect AWS Security Agent ai repository Bitbucket Cloud per abilitare la revisione del codice, la modellazione delle minacce, i test di penetrazione e le funzionalità di correzione automatica. Prima di iniziare, esamina the section called "Come funzionano le integrazioni con Agent Spaces" per capire come una registrazione viene riutilizzata tra Agent Spaces e condivisa tra le funzionalità.

L'integrazione con Bitbucket serve a diversi scopi:

- Revisione del codice: analizza automaticamente le modifiche al codice in ogni pull request rispetto ai requisiti di sicurezza dell'organizzazione ed esegui scansioni complete dell'archivio su richiesta
- Modellazione delle minacce: consente di comprendere le applicazioni analizzando il codice sorgente, i flussi di dati e l'architettura
- Contesto dei test di penetrazione: fornisce la comprensione delle applicazioni per i test di penetrazione
- Correzione automatizzata: invia richieste pull con correzioni per le vulnerabilità scoperte durante le valutazioni di sicurezza

La connessione di Bitbucket ad AWS Security Agent richiede l'installazione dell'app AWS Security Agent Forge sul tuo sito Atlassian e il completamento del flusso di autorizzazione OAuth.

> **Note**
>
> AWS Security Agent supporta solo Bitbucket Cloud. Bitbucket Server e Bitbucket Data Center non sono supportati.

Come funziona l'integrazione con Bitbucket

L'analisi delle pull request avviene all'interno di Bitbucket. Dopo aver installato l'app Forge, collegato i repository e abilitato i commenti di revisione del codice nella Console di gestione AWS, AWS Security Agent analizza automaticamente le modifiche in ogni nuova pull request (una scansione differenziale del solo codice modificato) e pubblica i risultati come commenti di pull request.

Puoi creare ed eseguire revisioni complete del codice, che scansionano l'intera base di codice di un repository, nell'applicazione Web AWS Security Agent, non in Bitbucket.

I test di penetrazione e la modellazione delle minacce vengono avviati all'interno dell'applicazione Web AWS Security Agent. Gli utenti specificano i domini di destinazione e selezionano i repository connessi per fornire il contesto dell'applicazione.

> **Note**
>
> La correzione automatica non è disponibile per gli archivi pubblici di Bitbucket per evitare di rivelare le vulnerabilità prima che vengano corrette.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Un'area di lavoro Bitbucket Cloud con accesso da amministratore
- Un account Atlassian con privilegi di amministratore del sito
- Autorizzazioni per configurare le integrazioni nella console di gestione di AWS Security Agent

> **Important**
>
> Un sito Atlassian può essere associato a un solo account AWS per regione. Se devi connettere lo stesso sito Bitbucket ad AWS Security Agent in un altro account AWS all'interno della stessa regione, devi prima rimuovere l'integrazione esistente.

> **Note**
>
> I prezzi dell'app Atlassian Forge si applicano a questa integrazione. Per ulteriori informazioni, consulta i prezzi della piattaforma Forge nella documentazione di Atlassian.

Registra una connessione Bitbucket

1. Nella Console di gestione di AWS Security Agent, vai a Integrazioni.
2. Scegli Aggiungi integrazione.
3. Seleziona Bitbucket, quindi scegli Avanti.
4. Installa l'app AWS Security Agent Forge nel tuo spazio di lavoro Bitbucket seguendo le istruzioni visualizzate sullo schermo. Dopo l'installazione, copia l'ID di installazione. Per informazioni, consulta the section called "Trova il tuo ID di installazione Atlassian".
5. Nel campo ID di installazione, incolla l'ID di installazione che hai copiato da Bitbucket.
6. Nel campo Bitbucket workspace, inserisci il tuo Bitbucket workspace slug, ad esempio. `acme-corp`
7. Seleziona Authorize (Autorizza).

   Verrai reindirizzato ad Atlassian per autorizzare AWS Security Agent ad accedere al tuo spazio di lavoro Bitbucket. Una volta completata l'autorizzazione, torni alla console.
8. Nella sezione Dettagli del registro, inserisci un nome di registrazione per questa connessione. I caratteri validi sono lettere, numeri, punti, caratteri di sottolineatura e trattini.
9. Scegli Connetti.

> **Note**
>
> Ritardo di fornitura dopo la connessione
>
> Dopo aver scelto Connect, il provisioning sul lato Atlassian può richiedere alcuni minuti. Durante questo periodo, l'integrazione segnala uno stato in sospeso. Se si tenta di selezionare i repository o di abilitare la revisione del codice prima del completamento del provisioning, è possibile che venga visualizzato un messaggio che indica che l'installazione non è ancora disponibile. Attendere qualche minuto e riprovare.

Risolvi i problemi di integrazione con Bitbucket

Se riscontri problemi durante il processo di integrazione di Bitbucket, utilizza la seguente guida per risolvere i problemi più comuni.

Impossibile completare la registrazione

Se il processo di registrazione viene interrotto (browser chiuso, timeout della sessione), l'app Forge può essere installata sul tuo sito Atlassian ma non registrata nella Console AWS.

Risoluzione

- Torna alla console AWS Security Agent e riavvia il processo di integrazione.
- L'app Forge rimane installata e non deve essere reinstallata.

Sito già connesso a un altro account AWS

Caratteristiche

- Errore che indica che il sito Atlassian è già associato a un altro account

Risoluzione

- Un sito Atlassian può essere collegato a un solo account AWS per regione.
- Identifica quale account AWS ha l'integrazione esistente e usa quell'account, oppure rimuovi prima l'integrazione esistente.

L'installazione non è disponibile

Caratteristiche

- Quando selezioni i repository o abiliti la revisione del codice, viene visualizzato un messaggio che indica che l'installazione di Bitbucket è in stato`PENDING_INSTALLATION`, ma non. `AVAILABLE`

Risoluzione

- L'installazione è ancora in fase di provisioning sul lato Atlassian. Il provisioning viene normalmente completato entro pochi minuti. Attendi qualche minuto, quindi riprova.

- Se lo stato non diventa disponibile dopo alcuni minuti, rimuovi l'integrazione e registrala nuovamente. Prima di registrarti nuovamente, disinstalla l'app Forge dal tuo spazio di lavoro Bitbucket. Per istruzioni, consulta Rimuovere un'integrazione Bitbucket. Se ti registri nuovamente senza disinstallare la precedente app Forge, l'installazione potrebbe rimanere bloccata.

Fasi successive

Dopo aver collegato Bitbucket a AWS Security Agent:

- Accedi all'Agent Space in cui desideri utilizzare questi repository
- Scegli Abilita la revisione del codice o Setup penetration testing per connettere repository specifici al tuo Agent Space
- Abilita la correzione del codice per consentire ad AWS Security Agent di inviare richieste pull con correzioni di vulnerabilità

Rimuovi un'integrazione Bitbucket

Rimuovi un'integrazione Bitbucket quando non hai più bisogno di AWS Security Agent per accedere ai repository da uno specifico spazio di lavoro Bitbucket.

Prerequisiti per la rimozione

Prima di rimuovere un'integrazione Bitbucket:

- Verifica a quali Agent Spaces sono collegati i repository da questa integrazione
- Comprendi l'impatto: la rimozione interromperà la revisione del codice, il contesto dei test di penetrazione, la modellazione delle minacce e la correzione automatica per tutti gli archivi connessi

Fase 1: rimuovere l'integrazione da AWS Security Agent

1. Nella Console di gestione di AWS Security Agent, vai a Integrazioni.
2. Individua l'integrazione Bitbucket che desideri rimuovere.
3. Seleziona l'integrazione.
4. Scegli Rimuovi.
5. Rivedi la finestra di dialogo di conferma e scegli Conferma rimozione.

Passaggio 2: disinstalla l'app Forge

Dopo aver rimosso l'integrazione da AWS Security Agent, disinstalla l'app Forge dal tuo sito Atlassian:

1. In Bitbucket, accedi alle impostazioni di Workspace.
2. Seleziona Forge Apps.
3. Individua Connect with AWS Security Agent.
4. Scegliere Uninstall (Disinstalla).

> **Important**
>
> L'app Forge non viene disinstallata automaticamente
>
> La rimozione dell'integrazione nella console AWS Security Agent non disinstalla l'app Forge dal tuo sito Atlassian. Se prevedi di registrare nuovamente lo stesso spazio di lavoro Bitbucket, devi prima disinstallare l'app Forge. In caso contrario, la nuova installazione potrebbe rimanere bloccata in uno stato in sospeso.

Connetti AWS Security Agent a Confluence

Connect AWS Security Agent a Confluence Cloud per fornire un contesto documentale per le valutazioni della sicurezza. A differenza dei fornitori di codice, Confluence funge da fonte di documentazione che fornisce modelli di minaccia, documenti di architettura, specifiche delle API e altro materiale che migliora la qualità delle revisioni di sicurezza. Prima di iniziare, esamina the section called "Come funzionano le integrazioni con Agent Spaces" per capire come viene riutilizzata una registrazione in Agent Spaces.

L'integrazione con Confluence serve a diversi scopi:

- Contesto di revisione del progetto: fornisce documenti architettonici e specifiche di progettazione per le revisioni dei progetti di sicurezza
- Modellazione delle minacce: fornisce i modelli di minaccia esistenti e la documentazione di sistema per l'analisi delle minacce
- Contesto dei test di penetrazione: fornisci la documentazione applicativa per una comprensione più approfondita durante i test di penetrazione

La connessione di Confluence ad AWS Security Agent richiede l'installazione dell'app AWS Security Agent Forge sul tuo sito Atlassian e il completamento del flusso di autorizzazione OAuth.

> **Note**
>
> AWS Security Agent supporta solo Confluence Cloud. Confluence Data Center e Confluence Server non sono supportati.

Come funziona l'integrazione con Confluence

Confluence è un fornitore di documentazione piuttosto che un fornitore di codice sorgente. Dopo aver installato l'app Forge e collegato spazi o pagine nella Console di gestione AWS, AWS Security Agent può accedere ai contenuti Confluence per fornire un contesto durante le valutazioni di sicurezza.

AWS Security Agent legge il contenuto delle pagine per comprendere l'architettura dell'applicazione, i requisiti di sicurezza e le decisioni di progettazione. Questo contesto migliora la qualità e la pertinenza dei risultati di sicurezza durante le revisioni di progettazione, le revisioni del codice e i test di penetrazione.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Un sito Confluence Cloud con accesso amministrativo
- Un account Atlassian con privilegi di amministratore del sito
- Autorizzazioni per configurare le integrazioni nella console di gestione di AWS Security Agent

> **Important**
>
> Un sito Atlassian può essere associato a un solo account AWS per regione. Se devi connettere lo stesso sito Confluence ad AWS Security Agent in un altro account AWS all'interno della stessa regione, devi prima rimuovere l'integrazione esistente.

> **Note**
>
> I prezzi dell'app Atlassian Forge si applicano a questa integrazione. Per ulteriori informazioni, consulta i prezzi della piattaforma Forge nella documentazione di Atlassian.

Registra una connessione Confluence

1. Nella Console di gestione di AWS Security Agent, vai a Integrazioni.
2. Scegli Aggiungi integrazione.
3. Seleziona Confluence, quindi scegli Avanti.
4. Installa l'app AWS Security Agent Forge nel tuo sito Atlassian seguendo le istruzioni sullo schermo. Dopo l'installazione, copia l'ID di installazione. Per informazioni, consulta the section called "Trova il tuo ID di installazione Atlassian".
5. Nel campo URL del sito Confluence, inserisci l'URL del tuo sito, ad esempio. `https://acme.atlassian.net`
6. Nel campo ID di installazione, incolla l'ID di installazione che hai copiato da Confluence.
7. Seleziona Authorize (Autorizza).

   Verrai reindirizzato ad Atlassian per autorizzare AWS Security Agent ad accedere al tuo sito Confluence. Una volta completata l'autorizzazione, torni alla console.
8. Nella sezione Dettagli del registro, inserisci un nome di registrazione per questa connessione. I caratteri validi sono lettere, numeri, punti, caratteri di sottolineatura e trattini.
9. Scegli Connetti.

Seleziona le pagine per un Agent Space

Dopo aver registrato l'integrazione con Confluence, collega pagine specifiche a un Agent Space. La selezione di una pagina concede ad AWS Security Agent l'accesso in lettura (fetch) ai contenuti di quella pagina. Non sono disponibili opzioni di funzionalità per pagina: l'agente legge ogni pagina connessa. Nella fase di revisione della procedura guidata di connessione, puoi rimuovere tutte le pagine a cui non desideri che l'agente acceda.

Risolvi i problemi di integrazione con Confluence

Se riscontri problemi durante il processo di integrazione di Confluence, utilizza la seguente guida per risolvere i problemi più comuni.

Impossibile completare la registrazione

Se il processo di registrazione viene interrotto, l'app Forge potrebbe essere installata sul tuo sito Atlassian ma non registrata nella console AWS.

Risoluzione

- Torna alla console AWS Security Agent e riavvia il processo di integrazione.
- L'app Forge rimane installata e non deve essere reinstallata.

L'app Forge è stata disinstallata da Atlassian

Se l'app AWS Security Agent Forge viene disinstallata dal tuo sito Atlassian mentre l'integrazione esiste ancora in AWS Security Agent:

Caratteristiche

- L'integrazione viene visualizzata nella console AWS ma non può accedere ai contenuti Confluence
- Errori durante il tentativo di elencare o leggere le pagine

Risoluzione

- Reinstalla l'app Forge dall'Atlassian Marketplace
- Se il problema persiste, rimuovi l'integrazione nella console AWS e registrati nuovamente

Sito già connesso a un altro account AWS

Risoluzione

- Un sito Atlassian può essere collegato a un solo account AWS per regione.
- Identifica quale account AWS ha l'integrazione esistente e usa quell'account, oppure rimuovi prima l'integrazione esistente.

Fasi successive

Dopo aver collegato Confluence a AWS Security Agent:

- Vai all'Agent Space in cui desideri utilizzare questa documentazione
- Seleziona pagine specifiche da includere come contesto per le revisioni del progetto e i test di penetrazione
- Carica documentazione aggiuntiva tramite S3, se necessario (vedi) the section called "Fornisci risorse agli agenti da un bucket S3"

Rimuovere un'integrazione Confluence

Rimuovi un'integrazione Confluence quando non hai più bisogno di AWS Security Agent per accedere alla documentazione da un sito Confluence specifico.

Prerequisiti per la rimozione

Prima di rimuovere un'integrazione Confluence:

- Verifica a quali Agent Spaces sono collegate pagine da questa integrazione
- Comprendi l'impatto: la rimozione interromperà il contesto della documentazione per le revisioni della progettazione, i test di penetrazione e la modellazione delle minacce in tutti gli Agent Spaces che utilizzano i contenuti di questa integrazione

Fase 1: rimuovere l'integrazione da AWS Security Agent

1. Nella Console di gestione di AWS Security Agent, vai a Integrazioni.
2. Individua l'integrazione Confluence che desideri rimuovere.
3. Seleziona l'integrazione.
4. Scegli Rimuovi.
5. Rivedi la finestra di dialogo di conferma e scegli Conferma rimozione.

Passo 2: Disinstalla l'app Forge (opzionale)

Dopo aver rimosso l'integrazione da AWS Security Agent, puoi opzionalmente disinstallare l'app Forge dal tuo sito Atlassian:

1. In Confluence, accedi all'amministrazione di Confluence.
2. Seleziona App.
3. Individua Connect with AWS Security Agent.
4. Scegliere Uninstall (Disinstalla).

Connect al controllo del codice sorgente ospitato privatamente

> **Important**
>
> Le connessioni private sono disponibili in anteprima per AWS Security Agent e sono soggette a modifiche.

AWS Security Agent può connettersi a sistemi di controllo del codice sorgente in esecuzione su reti private, come GitLab Self-Managed istanze ed GitHub Enterprise Server. Le connessioni private utilizzano Amazon VPC Lattice per stabilire una connettività sicura tra AWS Security Agent e l'infrastruttura privata senza esporre i sistemi alla rete Internet pubblica.

Come funzionano le connessioni private

Una connessione privata crea un percorso di rete sicuro tra AWS Security Agent e una risorsa di destinazione nel tuo VPC. Sotto il cofano, AWS Security Agent utilizza Amazon VPC Lattice per stabilire questa connettività. VPC Lattice è un servizio di rete di applicazioni AWS per connettere, proteggere e monitorare il traffico tra i servizi tra VPC e account, senza dover gestire l'infrastruttura di rete sottostante.

Quando crei una connessione privata:

1. Fornisci il VPC, le sottoreti e (facoltativamente) i gruppi di sicurezza che dispongono di connettività di rete al servizio di destinazione.
2. AWS Security Agent crea un gateway di risorse gestito dai servizi e fornisce interfacce di rete elastiche (ENI) nelle sottoreti specificate.
3. L'agente utilizza il gateway di risorse per indirizzare il traffico verso l'indirizzo IP o il nome DNS del servizio di destinazione tramite il percorso di rete privato.

Service-managed rispetto a connessioni private autogestite

AWS Security Agent supporta due modalità per le connessioni private:

Service-managed(consigliato per configurazioni semplici):

- AWS Security Agent crea e gestisce il gateway di risorse VPC Lattice per te.
- Il servizio di destinazione deve essere in esecuzione nello stesso account AWS in cui viene creato l'Agent Space.
- Non può estendersi su più account AWS.

Self-managed(per configurazioni avanzate o tra più account):

- Puoi creare e gestire la tua configurazione di risorse VPC Lattice.
- Fornisci l'Amazon Resource Name (ARN) della tua configurazione di risorse esistente.
- Supporta l'accesso tra account (il cliente gestisce la rete tra account).

Prerequisiti

Prima di creare una connessione privata, verifica di avere:

- Un Agent Space attivo
- Un servizio di destinazione raggiungibile privatamente (GitLab Self-Managed o GitHub Enterprise Server) con un indirizzo IP privato o un nome DNS noto
- Il servizio di destinazione deve servire il traffico HTTPS con una versione TLS minima di 1.2
- Sottoreti nel tuo VPC (1-20 sottoreti). Ti consigliamo di selezionare sottoreti in più zone di disponibilità per un'elevata disponibilità.
- (Facoltativo) Gruppi di sicurezza per controllare il traffico verso gli ENI (fino a 5)

> **Note**
>
> Le seguenti zone di disponibilità non sono supportate da VPC Lattice:`use1-az3`,,,`usw1-az2`,`apne1-az3`,, `apne2-az2euc1-az2`,`euw1-az4`. `cac1-az3` `ilc1-az2`

> **Note**
>
> Le connessioni private sono risorse a livello di account. Dopo aver creato una connessione privata, puoi riutilizzarla su più integrazioni e Agent Spaces che devono raggiungere lo stesso host.

> **Note**
>
> Quando selezioni una connessione privata per un provider che utilizza l'autenticazione OAuth, la connessione privata si applica sia all'endpoint del provider che all'endpoint di scambio di token. Assicurati che la connessione privata sia configurata con un indirizzo host in grado di indirizzare il traffico verso entrambi gli endpoint.

Crea una connessione privata

1. Nella Console di gestione di AWS Security Agent, vai a Integrazioni.
2. Scegli la scheda Connessioni private.
3. Scegli Crea connessione privata.
4. In Dettagli di connessione, inserisci un nome. I nomi possono contenere lettere minuscole, numeri e trattini e devono iniziare e terminare con una lettera o un numero.
5. Nella sezione Dettagli della connessione, scegli in che modo AWS Security Agent si connette al servizio di destinazione:
   - Per fare in modo che AWS Security Agent crei e gestisca la connessione, lascia deselezionata l'opzione Usa configurazione delle risorse esistente, quindi completa le sezioni Resource location, Access control e Service target details.
   - Per eseguire il routing attraverso una configurazione di risorse VPC Lattice che hai già creato, seleziona Usa la configurazione delle risorse esistenti, quindi completa la sezione Configurazione delle risorse esistenti. Le sezioni gestite dai servizi non si applicano.
6. (Service-managed) In Ubicazione della risorsa:
   a. Seleziona il VPC in cui si trova la tua risorsa.
   b. Seleziona una o più sottoreti. Consigliamo di selezionare le sottoreti in almeno due zone di disponibilità.
   c. (Facoltativo) Seleziona un tipo di indirizzo IP (IPv4, IPv6 o Dual stack).

7. (Service-managed) In Controllo degli accessi:
   a. Seleziona i gruppi di sicurezza associati alle risorse connesse.
   b. (Facoltativo) In Configurazione avanzata, inserisci gli intervalli di porte, ad esempio fino a 11 porte o intervalli TCP separati da virgole. `443, 8080-8090`
8. (Service-managed) In Dettagli dell'obiettivo del servizio:
   a. Nel campo Indirizzo host, inserisci il nome host DNS o l'indirizzo IP del servizio di destinazione.
   b. Per la risoluzione DNS, seleziona Pubblico per un indirizzo host risolvibile pubblicamente o In VPC (DNS privato) per un indirizzo risolvibile solo all'interno del VPC.
   c. (Facoltativo) Nel campo Chiave pubblica del certificato, inserisci la chiave PEM-encoded pubblica se la destinazione utilizza un certificato autofirmato o un'autorità di certificazione privata. Ciò consente ad AWS Security Agent di fidarsi della connessione TLS.
9. (Self-managed) In Configurazione delle risorse esistenti, per Configurazione delle risorse, seleziona una configurazione di risorsa VPC Lattice dall'elenco o inserisci un ID di configurazione della risorsa (che inizia con `rcfg-`) o il relativo ARN. L'elenco mostra le configurazioni delle risorse nella regione corrente.
10. Scegli Crea connessione.

    Lo stato della connessione cambia in Creazione in corso. Questa operazione può richiedere fino a 10 minuti. Al termine, lo stato diventa Disponibile.

Usa una connessione privata con un'integrazione

Quando registri un' GitLab Self-Managed integrazione con GitHub Enterprise Server, seleziona Connetti all'endpoint utilizzando una connessione privata, quindi scegli la tua connessione dall'elenco Connessione privata. AWS Security Agent indirizza il traffico verso il provider tramite tale connessione. Nell'elenco vengono visualizzate solo le connessioni con lo stato Disponibile.

Puoi anche scegliere Crea una connessione privata durante la registrazione. AWS Security Agent conserva la bozza di registrazione durante la creazione della connessione, quindi ti riporta al flusso di registrazione.

Sicurezza

- Nessuna esposizione pubblica a Internet: tutto il traffico rimane sulla rete AWS.
- Customer-controlled gruppi di sicurezza: gestisci le regole del traffico in entrata e in uscita.

- Service-linked ruolo con privilegio minimo: AWS Security Agent utilizza un ruolo collegato al servizio limitato alle risorse contrassegnate. `AWSSecurityAgentManaged`

> **Note**
>
> Se la tua organizzazione dispone di policy di controllo dei servizi (SCP) che limitano le azioni dell'API VPC Lattice, il gateway di risorse gestito dai servizi viene creato tramite un ruolo collegato al servizio. Assicurati che i tuoi SCP consentano le azioni necessarie per il ruolo collegato al servizio.

Verifica una connessione privata

Dopo che la connessione privata ha raggiunto lo stato Disponibile, verifica la connettività:

- Assicurati che il servizio di destinazione sia in esecuzione e accetti connessioni sulla porta prevista
- Verifica che i gruppi di sicurezza collegati agli ENI consentano il traffico in uscita sulla porta di destinazione
- Verifica che il gruppo di sicurezza del tuo servizio consenta il traffico in entrata dagli IP del piano dati VPC Lattice all'interno dell'intervallo VPC CIDR
- Verifica che le tabelle di routing delle sottoreti consentano il traffico tra le sottoreti ENI e il tuo servizio

Eliminare una connessione privata

1. Nella console AWS Security Agent, vai a Integrazioni.
2. Scegli la scheda Connessioni private.
3. Seleziona la connessione privata che desideri eliminare.
4. Scegli Elimina.

> **Important**
>
> Non è possibile eliminare una connessione privata attualmente utilizzata da un'integrazione. Rimuovi prima l'integrazione, quindi elimina la connessione privata.

Fasi successive

- the section called "Connect AWS Security Agent a GitLab Self-Managed"- Connect un' GitLab istanza privata
- the section called "Connect AWS Security Agent a GitHub Enterprise Server"- Connect un GitHub Enterprise Server privato

Connect agent a risorse VPC private

Se l'applicazione su cui desideri eseguire un test di penetrazione non è disponibile sulla rete Internet pubblica, devi fornire ad AWS Security Agent una configurazione VPC. AWS Security Agent utilizzerà questa configurazione VPC, tra cui un VPC, una sottorete e gruppi di sicurezza, per accedere all'applicazione.

> **Note**
>
> Quando si testano gli endpoint in un VPC privato, sono consentiti solo gli endpoint che si risolvono in IP in intervalli IP privati noti (vedi Blocchi VPC CIDR per ulteriori informazioni). Sono consentiti i seguenti intervalli IPv4 e IPv6:
>
> ```
> 10.0.0.0/8
> 172.16.0.0/12
> 192.168.0.0/16
> fd00::/8
> ```

> **Note**
>
> Durante la connessione a una sottorete, AWS Security Agent creerà un'ENI (Elastic Network Interface) nella sottorete configurata per il test di penetrazione. Questo ENI non ha un indirizzo IP pubblico associato, il che significa che non può comunicare con i gateway Internet VPC nelle sottoreti pubbliche. Se il tuo penetration test richiede un accesso aperto a Internet, utilizza invece una sottorete privata con un gateway NAT VPC associato

Concedi ad AWS Security Agent l'accesso generale a un VPC dalla Console di gestione AWS. Nell'app web Security Agent, gli utenti selezionano la configurazione specifica per un test di penetrazione.

Per aggiungere un VPC nello spazio degli agenti

1. Vai alla pagina di panoramica di Agent Space
2. Seleziona Azioni, quindi Modifica la configurazione del test di penetrazione
3. Sotto l'intestazione VPC, specifica i gruppi VPC, sottoreti e sicurezza

Puoi aggiungere fino a 5 VPC.

Autorizzazioni richieste per il ruolo del servizio Agent Space

Per eseguire un test di penetrazione con un VPC, il ruolo del servizio Agent Space deve includere le seguenti autorizzazioni:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkInterfacePermission",
      "Resource": "arn:aws:ec2:{{region}}:{{accountId}}:network-interface/*",
      "Condition": {
        "ArnEquals": {
```

```
          "ec2:Subnet": [
            "arn:aws:ec2:{{region}}:{{accountId}}:subnet/[[subnetIds]]"
          ]
        }
      }
    }
  ]
}
```

Per selezionare una configurazione VPC specifica per un test di penetrazione nell'app Web Security Agent

1. Vai alla pagina di panoramica dei test di penetrazione
2. Seleziona il test di penetrazione per cui devi aggiungere la configurazione VPC, quindi scegli Modifica dettagli pentest
3. Seleziona Avanti per accedere alla sezione Risorse VPC
4. Seleziona i gruppi VPC, Subnet e Security
5. Seleziona Avanti per raggiungere l'ultima sezione e Salva il test di penetrazione

> **Note**
>
> Cross-account i test di penetrazione sono attualmente supportati per le risorse VPC (sottoreti e gruppi di sicurezza) condivise utilizzando AWS Resource Access Manager. I segreti di Secrets Manager e le funzioni Lambda utilizzate per le credenziali di autenticazione devono essere configurati nello stesso account AWS utilizzato per la configurazione di AWS Security Agent.

Esecuzione di un test di penetrazione sulle risorse VPC in un altro account AWS

Puoi eseguire test di penetrazione sulle risorse VPC condivise con il tuo account utilizzando AWS Resource Access Manager. Entrambi gli account devono far parte della stessa AWS Organization.

1. (Facoltativo) Abilita la condivisione automatica delle risorse per la tua organizzazione AWS

```
aws ram enable-sharing-with-aws-organization
```

2. Utilizzando le credenziali dell'account AWS che possiede le risorse VPC, condividi le risorse della sottorete e del gruppo di sicurezza con l'account proprietario del penetration test

```
aws ram create-resource-share \
    --name SharePentestResources \
    --resource-arns <subnet ARN> <security group ARN> \
    --principals <penetration test owner account ID>
```

3. Vai alla pagina di panoramica di Agent Space
4. Seleziona Penetration test e individua il nome del ruolo del servizio
5. Verifica che il ruolo IAM conceda l'accesso alle risorse VPC condivise
6. Seleziona Azioni, quindi Modifica la configurazione del test di penetrazione
7. Sotto l'intestazione VPC, specifica il VPC condiviso, le sottoreti e i gruppi di sicurezza e salva la configurazione aggiornata.
8. Vai alla pagina di panoramica dei test di penetrazione sull'app Web AWS Security Agent
9. Seleziona il test di penetrazione per cui devi aggiungere la configurazione VPC, quindi scegli Modifica dettagli pentest
10. Aggiorna il test di penetrazione per utilizzare le risorse VPC condivise

Configurazione delle funzionalità

Abilita e configura i test di penetrazione, la revisione del codice e la modellazione delle minacce per i tuoi Agent Spaces, tra cui la riparazione, le sorgenti S3 e i domini di destinazione.

Abilita il test di penetrazione

Configura AWS Security Agent per eseguire test di penetrazione autonomi sulle tue applicazioni. Questa configurazione consente ad AWS Security Agent di accedere alle risorse AWS, verificare la proprietà del dominio ed eseguire test di sicurezza completi che identificano le vulnerabilità sfruttabili nelle applicazioni Web e nelle API.

L'abilitazione dei test di penetrazione consente ad AWS Security Agent di convalidare continuamente la sicurezza delle applicazioni senza i ritardi dei test manuali. Configurando le integrazioni AWS necessarie, garantisci che AWS Security Agent possa testare applicazioni pubbliche e private, registrare i risultati e accedere alle credenziali per i test autenticati. CloudWatch

In questa procedura, configurerai i domini di destinazione, opzionalmente configurerai VPC, CloudWatch registrazione, archiviazione delle credenziali e funzioni Lambda per i test, configurerai le integrazioni S3 per fornire un contesto aggiuntivo e configurerai l'accesso al servizio tramite i ruoli IAM.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Account AWS con autorizzazioni amministrative per creare ruoli IAM
- Capacità di verifica della proprietà del dominio (modifica dei record DNS o HTTP)
- Domini o applicazioni di destinazione da testare
- (Facoltativo) Dettagli sulla configurazione VPC in caso di test di applicazioni private
- (Facoltativo) Bucket S3 se fornisce artefatti aggiuntivi ad AWS Security Agent

Fase 1: Configurazione del dominio

Nel primo passaggio della procedura guidata, specifica i domini di destinazione che desideri testare e in che modo AWS Security Agent deve verificare la proprietà.

1. Nella sezione Domini Target, inserisci il tuo dominio nel campo Dominio.
2. Seleziona un metodo di verifica:
   - DNS_TXT: dimostra la proprietà del dominio aggiungendo un record TXT alla configurazione DNS del dominio.
   - HTTP_ROUTE: dimostra la proprietà del dominio ospitando un file di verifica su un URL specifico del tuo dominio.
   - PRIVATE_VPC - Utilizzabile solo per test di penetrazione VPC privati. Verifica che il dominio si risolva in un IP in un intervallo CIDR privato
   - Per ulteriori informazioni, consulta the section called “Abilita un dominio applicativo per i test di penetrazione”.
3. Scegli Aggiungi un altro dominio per aggiungere altri domini (fino a 5 in totale).
4. Scegli Avanti per procedere alla verifica del dominio.

Fase 2: Verifica i domini

Nel secondo passaggio della procedura guidata, verifica la proprietà di ogni dominio configurato. AWS Security Agent richiede una proprietà verificata prima di poter eseguire test di penetrazione.

1. Esamina i domini elencati nella tabella dei domini di Target.
2. Per ogni dominio, selezionalo e attiva la verifica in base al metodo scelto:
   - Domini Route 53 (stesso account AWS): scegli One-click la verifica. AWS Security Agent crea automaticamente il record DNS e completa la verifica.
   - DNS TXT (altri provider DNS): copia il token di verifica, aggiungi il record TXT con il tuo registrar DNS, quindi seleziona il dominio e scegli Verifica.
   - Percorso HTTP: posiziona il token di verifica sul percorso di percorso richiesto sul tuo server web, quindi seleziona il dominio e scegli Verifica. Per informazioni dettagliate, vedi the section called "Abilita un dominio applicativo per i test di penetrazione".
3. Scegli Avanti per procedere alla configurazione opzionale.

> **Note**
>
> Sub-domains di un dominio verificato non è necessaria la verifica individuale quando si utilizza la verifica del percorso DNS, TXT o HTTP. Per la verifica VPC privato, il nome di dominio dell'endpoint di destinazione deve corrispondere al nome di dominio completo configurato per la verifica.

> **Note**
>
> Per i domini privati all'interno di un VPC, puoi procedere anche se lo stato di verifica del dominio è IRRAGGIUNGIBILE. AWS Security Agent tenterà la verifica del dominio per gli endpoint privati all'inizio di ogni esecuzione di pentest.

Fase 3: (Facoltativo) Configurare funzionalità aggiuntive

Il terzo passaggio della procedura guidata consente di configurare risorse AWS opzionali per espandere l'ambito dei test di penetrazione. Tutte le sezioni di questo passaggio sono opzionali e ridotte per impostazione predefinita.

(Facoltativo) Configurare le impostazioni VPC

Se prevedi di testare domini di destinazione privati ospitati all'interno di un VPC, configura le impostazioni VPC per AWS Security Agent. Questa sezione è facoltativa ed è compressa per impostazione predefinita.

1. Espandi la sezione VPC.
2. Nel menu a discesa VPC, seleziona il VPC che ospita i tuoi domini di destinazione privati.
3. Nel menu a discesa Subnet, seleziona le sottoreti VPC che AWS Security Agent deve utilizzare:

> **Tip**
>
> Per un'elevata disponibilità, seleziona più sottoreti da più zone di disponibilità. Assicurati che le tue sottoreti includano un gateway NAT per la connettività in uscita.

4. Nel menu a discesa Security group, seleziona i gruppi di sicurezza VPC che AWS Security Agent deve utilizzare:

> **Important**
>
> Assicurati che i tuoi gruppi di sicurezza consentano le connessioni in uscita per consentire ad AWS Security Agent di eseguire test di penetrazione.

(Facoltativo) Configura la registrazione CloudWatch

Configura CloudWatch per archiviare i log dei test di penetrazione. Questa sezione è facoltativa ed è compressa per impostazione predefinita.

1. Espandi la sezione dei CloudWatch registri.
2. Nel menu a discesa Gruppi di log, seleziona i gruppi di log esistenti CloudWatch
3. Se non seleziona alcun gruppo di log, AWS Security Agent creerà un gruppo di log denominato `/aws/securityagent/<agent name>/<pentest id>` con le autorizzazioni appropriate.

> **Note**
>
> Assicurati che il tuo ruolo IAM disponga delle autorizzazioni per scrivere nel gruppo di CloudWatch log selezionato.

(Facoltativo) Configura Secrets per le credenziali di test

Se l'applicazione richiede credenziali di autenticazione per il test, AWS Security Agent può recuperarle in modo sicuro da AWS Secrets Manager. Questa sezione è facoltativa e compressa per impostazione predefinita.

1. Espandi la sezione Segreti.
2. Seleziona i segreti di AWS Secrets Manager che contengono le credenziali per la tua applicazione.
3. Quando configuri un penetration test nell'applicazione Web, puoi fare riferimento a questi segreti per i test autenticati.

> **Important**
>
> Le credenziali sono crittografate e archiviate in AWS Secrets Manager. Assicurati che il tuo ruolo IAM disponga delle autorizzazioni per accedere a Secrets Manager for AWS Security Agent per utilizzare queste credenziali durante i test.

(Facoltativo) Configurare le funzioni Lambda per le credenziali di test

Configura le funzioni Lambda in grado di fornire credenziali per l'applicazione durante i test. Questa sezione è facoltativa ed è compressa per impostazione predefinita.

1. Espandi la sezione Funzioni Lambda.
2. Seleziona le funzioni Lambda che possono fornire le credenziali di autenticazione per la tua applicazione.
3. AWS Security Agent invocherà queste funzioni durante i test di penetrazione per ottenere le credenziali in modo dinamico.

> **Note**
>
> Assicurati che il tuo ruolo IAM disponga delle autorizzazioni per richiamare le funzioni Lambda specificate. Le funzioni Lambda devono restituire le credenziali nel formato previsto per AWS Security Agent da utilizzare durante i test.

(Facoltativo) Configura il bucket S3

Fornisci i dettagli del bucket S3 se prevedi di caricare documenti o artefatti da fornire come input ad AWS Security Agent. Questa sezione è facoltativa ed è compressa per impostazione predefinita.

1. Espandi la sezione dei bucket S3.
2. Nel campo Bucket, inserisci o cerca il nome del tuo bucket S3.

> **Note**
>
> Puoi anche collegare i GitHub repository in un secondo momento o caricare i file direttamente nell'applicazione web. Le informazioni fornite possono garantire una copertura completa, ridurre i falsi positivi e fornire risultati utilizzabili.

(Facoltativo) Configura l'accesso al servizio

AWS Security Agent richiede un ruolo IAM per accedere alle risorse AWS (VPC, gruppi di CloudWatch log, Secrets Manager, funzioni Lambda, ecc.) per i test di penetrazione. Questa sezione è facoltativa ed è compressa per impostazione predefinita.

1. Espandi la sezione Accesso al servizio.
2. Per impostazione predefinita, AWS Security Agent utilizza un ruolo IAM predefinito con le autorizzazioni richieste per i test di penetrazione.
3. Per personalizzare il ruolo IAM, seleziona una delle seguenti opzioni:
   a. Crea un ruolo predefinito: AWS Security Agent crea automaticamente un nuovo ruolo IAM con le autorizzazioni necessarie
   b. Usa un ruolo di servizio esistente: seleziona un ruolo IAM esistente dal menu a discesa
4. Se utilizzi un ruolo esistente:
   a. Scegli il menu a discesa sotto Scegli un ruolo esistente

b. Seleziona il tuo ruolo IAM dall'elenco

c. Se necessario, scegli l'icona di aggiornamento per aggiornare l'elenco

> **Note**
>
> Il ruolo IAM predefinito include le autorizzazioni per l'accesso a risorse VPC, gruppi di log CloudWatch , Secrets Manager, funzioni Lambda e altri servizi necessari per i test di penetrazione. Si consiglia di utilizzare il ruolo IAM predefinito a meno che non si abbiano requisiti di sicurezza specifici.

Fase 4: Salvare e abilitare i test di penetrazione

Dopo aver configurato tutte le impostazioni richieste, abilita i test di penetrazione per il tuo agente AWS Security Agent.

1. Rivedi tutte le sezioni di configurazione per garantire l'accuratezza.
2. Scegli Save (Salva).
3. AWS Security Agent convalida la configurazione e crea le risorse AWS necessarie.

Fasi successive

Dopo aver abilitato i test di penetrazione:

- Configura gli ambiti dei test di penetrazione nell'applicazione Web AWS Security Agent
- Imposta le preferenze di notifica per i risultati dei test
- Esamina e rispondi ai risultati dei test di penetrazione non appena vengono scoperti
- (Facoltativo) Configura archivi aggiuntivi per la correzione dei risultati

Per ulteriori informazioni sull'esecuzione e la gestione dei penetration test, consulta la documentazione dell'applicazione web AWS Security Agent.

Abilita la revisione del codice pull request per i GitHub repository

La revisione del codice di pull request è ora configurata come parte della procedura guidata di configurazione della revisione del codice. Quando colleghi i GitHub repository al tuo Agent Space,

puoi abilitare i commenti pull request per i singoli repository in modo che AWS Security Agent analizzi automaticamente le richieste pull e pubblichi i risultati di sicurezza.

Per istruzioni di configurazione complete, consulta. the section called "Abilita la revisione del codice"

Per informazioni su come vengono visualizzati i risultati delle pull request GitHub e su come rispondervi, vederethe section called "Esamina i risultati sulla sicurezza del codice nelle richieste pull".

Abilita la revisione del codice

Configura Agent Space per abilitare la revisione del codice collegando il codice sorgente dai GitHub repository o dai bucket S3. La revisione del codice analizza il codice sorgente alla ricerca di vulnerabilità di sicurezza e conformità ai requisiti di sicurezza personalizzati dell'organizzazione.

L'impostazione delle configurazioni di revisione del codice è un'operazione dell'agente. Space-wide Le integrazioni e i bucket S3 che connetti sono condivisi tra diverse funzionalità, tra cui la revisione del codice e i test di penetrazione.

Dopo aver completato la configurazione, gli utenti possono creare ed eseguire revisioni del codice nell'applicazione Web AWS Security Agent per scansionare repository e sorgenti S3 alla ricerca di problemi di sicurezza.

> **Note**
>
> Se disponi già di GitHub repository collegati a Agent Space (ad esempio, tramite la configurazione dei test di penetrazione), la revisione del codice è già abilitata. Puoi saltare questa configurazione e andare direttamente all'applicazione web per creare revisioni del codice. Per informazioni, consulta the section called "Creare una revisione del codice".

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Uno spazio per agenti creato nella Console di gestione AWS (vedithe section called "Crea uno spazio per agenti")
- Almeno uno dei seguenti input di codice sorgente:
  - Un' GitHub organizzazione o un account utente con l' GitHub app AWS Security Agent installata (vedithe section called "Connect AWS Security Agent ai GitHub repository")

  - Un bucket S3 contenente il codice sorgente che desideri esaminare
- Autorizzazioni per configurare le integrazioni per Agent Space
- (Facoltativo) Almeno un requisito di sicurezza abilitato in un pacchetto di requisiti di sicurezza se prevedi di utilizzare la convalida dei requisiti di sicurezza (vedi) the section called "Gestisci i requisiti di sicurezza"

Accedi alla procedura guidata di configurazione per la revisione del codice

Passa alla configurazione di revisione del codice per Agent Space.

1. Nella console AWS Security Agent, seleziona il tuo Agent Space.
2. Scegli Enable code review da una delle seguenti posizioni:
   - La scheda di revisione del codice
   - Nella scheda Code review, quindi scegli Enable code review

> **Tip**
>
> Se desideri che AWS Security Agent risponda automaticamente al feedback sulla revisione del codice, abilita anche la correzione del codice. Per informazioni dettagliate, vedi the section called "Consenti agli utenti di avviare la correzione dei risultati dei test di penetrazione e della revisione del codice".

Verrai indirizzato alla procedura guidata per la revisione del codice di installazione e configurazione.

Fase 1: Connect integrazioni, repository e bucket

Nel primo passaggio della procedura guidata, collega gli input del codice sorgente e configura le impostazioni di revisione del codice. È necessario aggiungere almeno un GitHub repository o un bucket S3 per procedere.

> **Important**
>
> Le integrazioni e i bucket S3 configurati qui sono condivisi in tutto il tuo Agent Space. Le modifiche si applicano sia alle funzionalità di revisione del codice che ai test di penetrazione.

Connect GitHub repository

Aggiungi GitHub repository dalle tue GitHub organizzazioni o account utente autorizzati. Scegliendo Aggiungi si apre la GitHub procedura guidata Connect in due passaggi, in cui prima si selezionano i repository e poi si configurano le azioni che AWS Security Agent può intraprendere su ciascuno di essi.

1. Nella sezione Integrazioni connesse, scegli Aggiungi.
2. Seleziona la GitHub registrazione che contiene i repository che desideri esaminare.
3. Nella fase Connetti i GitHub repository, seleziona la casella di controllo per ogni repository che desideri connettere.
4. Scegli Avanti per andare a Gestisci le funzionalità.

> **Note**
>
> È possibile accedere ai repository collegati in sola lettura per l'analisi del codice durante la revisione del codice e i test di penetrazione. Nella fase successiva si configurano azioni di scrittura come la pubblicazione di commenti di recensione e l'apertura di richieste pull di correzione.

> **Note**
>
> Se non hai ancora registrato un' GitHub integrazione, scegli Impostazioni per accedere alla pagina Integrazioni in cui puoi autorizzare l'app AWS Security Agent GitHub . Per ulteriori informazioni, consulta the section called “Connect AWS Security Agent ai GitHub repository”.

Configura le funzionalità GitHub del repository

Nella fase di gestione delle funzionalità della GitHub procedura guidata Connect, scegli cosa può fare AWS Security Agent in ogni repository. I commenti di revisione del codice e la correzione del codice sono impostati indipendentemente per ogni repository.

1. Per ogni repository, attiva i commenti di revisione del codice per consentire ad AWS Security Agent di pubblicare i risultati di sicurezza come commenti sulle pull request.

2. Per ogni repository, attiva la correzione del codice per consentire ad AWS Security Agent di correggere i risultati. Se abilitata, gli utenti delle app Web possono richiedere richieste pull per correggere i risultati e gli autori delle pull request possono commentare `@AWS-Security-Agent fix all findings.` per far sì che l'agente risponda ai commenti di revisione.
3. Scegliete Salva per applicare le selezioni e tornare alla procedura guidata di configurazione per la revisione del codice.

Quando i commenti di revisione del codice sono abilitati per un repository:

- AWS Security Agent analizza automaticamente le richieste pull quando sono contrassegnate come «Pronte per la revisione». Le bozze di pull request non vengono analizzate.
- I risultati di sicurezza vengono pubblicati come commenti di revisione direttamente sulla pull request con indicazioni specifiche per la correzione.
- L'analisi utilizza le impostazioni di revisione del codice configurate (vulnerabilità di sicurezza, requisiti personalizzati o entrambi).

> **Note**
>
> I commenti sulle pull request sono disponibili solo per gli GitHub archivi privati.

Quando la correzione del codice è abilitata per un repository, gli utenti di app Web possono avviare la correzione sia per la revisione del codice che per i risultati dei test di penetrazione su tale repository e AWS Security Agent fornisce ogni correzione come pull request. Per ulteriori informazioni, consulta the section called “Consenti agli utenti di avviare la correzione dei risultati dei test di penetrazione e della revisione del codice”.

Per ulteriori informazioni su come vengono visualizzati i risultati delle pull request GitHub e su come rispondervi, consulta. the section called “Esamina i risultati sulla sicurezza del codice nelle richieste pull”

Aggiungi bucket S3

Aggiungi bucket S3 contenenti codice sorgente o risorse contestuali per la revisione del codice.

1. Nella sezione bucket S3, scegli Aggiungi risorsa S3.
2. Inserisci l'URI S3 per il bucket o il prefisso contenente il codice sorgente.

3. Scegliere Aggiungi.

> **Note**
>
> Puoi aggiungere fino a 10 risorse S3. I bucket S3 sono condivisi tra diverse funzionalità, tra cui la revisione del codice e i test di penetrazione.

> **Tip**
>
> Puoi aggiungere bucket S3 che contengono codice sorgente, file di configurazione, modelli infrastructure-as-code o altri elementi che desideri che AWS Security Agent analizzi per problemi di sicurezza.

Configura le impostazioni di revisione del codice

Configura i tipi di problemi di sicurezza che AWS Security Agent analizza durante le revisioni del codice. Questa impostazione si applica a tutti i repository e le fonti con la revisione del codice abilitata in questo Agent Space.

1. Nella sezione Impostazioni di revisione del codice, selezionate una delle seguenti opzioni:
   - Convalida dei requisiti di sicurezza: verifica se il codice è conforme ai requisiti di sicurezza che hai abilitato nei pacchetti dei requisiti di sicurezza.
   - Risultati delle vulnerabilità di sicurezza: identifica le vulnerabilità di sicurezza più comuni nel codice.
   - Requisiti di sicurezza e rilevazioni delle vulnerabilità: analizza il codice per verificare sia la conformità ai requisiti di sicurezza che hai abilitato sia le vulnerabilità di sicurezza più comuni. Questa è l'impostazione predefinita.

> **Note**
>
> Quando la convalida dei requisiti di sicurezza è abilitata, AWS Security Agent confronta il codice con i requisiti di sicurezza abilitati nei pacchetti dei requisiti di sicurezza. Se selezioni la convalida dei requisiti di sicurezza ma non hai almeno un requisito di sicurezza abilitato,

AWS Security Agent non identificherà i risultati basati sui requisiti. Per ulteriori informazioni sui requisiti di sicurezza, consulta the section called "Gestisci i requisiti di sicurezza".

1. Scegli Avanti per passare alle configurazioni opzionali.

Fase 2: configurazioni opzionali

Nel secondo passaggio della procedura guidata, configura le impostazioni opzionali di CloudWatch registrazione e accesso ai servizi per l'ambiente di revisione del codice.

(Facoltativo) Configura i registri CloudWatch

Configura i gruppi di CloudWatch log per acquisire e analizzare il comportamento delle applicazioni durante la revisione del codice.

1. Espandi la sezione CloudWatch dei log.
2. Nel menu a discesa Log Groups, seleziona uno o più gruppi di CloudWatch log esistenti dal tuo account AWS.

> **Note**
>
> Se non si seleziona un gruppo di log, AWS Security Agent crea automaticamente un gruppo di log predefinito per archiviare i log di esecuzione delle revisioni del codice.

(Facoltativo) Configura l'accesso al servizio

Configura il ruolo del servizio IAM che AWS Security Agent utilizza per accedere alle tue risorse AWS come i bucket e i CloudWatch log S3 per la revisione del codice.

1. Espandi la sezione Accesso al servizio.
2. Seleziona una delle seguenti opzioni:
   - Crea un ruolo predefinito: AWS Security Agent crea automaticamente un nuovo ruolo IAM con le autorizzazioni necessarie per la revisione del codice.
   - Usa un ruolo di servizio esistente: seleziona un ruolo IAM esistente dal menu a discesa.

3. Se utilizzi il ruolo predefinito, inserisci un nome per il ruolo di servizio. Il nome deve essere univoco per tutti i ruoli dell'account, utilizzare caratteri e `+=,.@-_` caratteri alfanumerici e non può includere spazi.

> **Note**
>
> Il nome del ruolo di servizio ha una lunghezza massima di 64 caratteri. Un ruolo di servizio viene creato automaticamente se non si seleziona un ruolo esistente.

1. Scegli Salva per completare la configurazione.

Dopo la configurazione

Dopo aver completato la procedura guidata di configurazione per la revisione del codice:

- La scheda di revisione del codice nella pagina Agent Space mostra lo stato Pronto.
- Gli utenti possono avviare l'applicazione Web e creare revisioni del codice per scansionare gli archivi collegati e le fonti S3.
- Puoi modificare la configurazione in qualsiasi momento selezionando Modifica configurazione nella scheda Code review.

Modifica la configurazione di revisione del codice

Per modificare la configurazione di revisione del codice dopo la configurazione iniziale:

1. Accedi al tuo Agent Space nella console AWS Security Agent.
2. Seleziona la scheda Code review.
3. Scegli Edit configuration (Modifica configurazione).
4. Aggiorna le integrazioni, i bucket S3, le impostazioni di revisione del codice, i CloudWatch log o l'accesso al servizio in base alle tue esigenze.
5. Scegli Save (Salva).

Fasi successive

Dopo aver configurato le configurazioni di revisione del codice:

- Avvia l'applicazione web per creare ed eseguire revisioni del codice (vedithe section called “Creare una revisione del codice”)
- Connect GitHub repository o bucket S3 aggiuntivi man mano che la tua codebase cresce
- Configura i pacchetti di requisiti di sicurezza per la convalida specifica dell'organizzazione (vedi) the section called “Gestisci i requisiti di sicurezza”
- Scopri come appaiono i risultati delle pull request in (vedi) GitHub the section called “Esamina i risultati sulla sicurezza del codice nelle richieste pull”

Abilita la modellazione delle minacce

Configura il tuo Agent Space per abilitare la modellazione delle minacce collegando gli archivi di codice sorgente e configurando le risorse AWS. La modellazione delle minacce analizza l'architettura dell'applicazione e identifica le minacce alla sicurezza dal codice sorgente, dai documenti di progettazione o da entrambi.

La configurazione delle configurazioni di modellazione delle minacce è un'operazione dell'agente. Space-wide Le integrazioni e i bucket S3 che connetti sono condivisi tra diverse funzionalità, tra cui la modellazione delle minacce, la revisione del codice e i test di penetrazione.

Dopo aver completato la configurazione, gli utenti possono creare ed eseguire modelli di minaccia nell'applicazione Web AWS Security Agent.

> **Note**
>
> Se disponi già di repository o bucket S3 collegati a Agent Space (ad esempio, tramite la revisione del codice o la configurazione dei test di penetrazione), la modellazione delle minacce potrebbe essere già abilitata. Puoi accedere direttamente all'applicazione web per creare un modello di minaccia. Per informazioni, consulta the section called “Crea un modello di minaccia”.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Uno spazio per agenti creato nella Console di gestione AWS (vedithe section called “Crea uno spazio per agenti”)

- Autorizzazioni per configurare le integrazioni per il tuo Agent Space
- (Facoltativo) Un' GitHuborganizzazione o Bitbucket con l'app AWS Security Agent installata (consulta Connetti AWS Security Agent ai GitHub repository, Connect AWS Security Agent ai GitLab repository o Connect AWS Security Agent ai repository Bitbucket) GitLab

Accedi alla procedura guidata di configurazione della modellazione delle minacce

Passa alla configurazione di modellazione delle minacce per Agent Space.

1. Nella console AWS Security Agent, seleziona il tuo Agent Space.
2. Scegli Configura modello di minaccia dalla scheda Modello di minaccia o dalla scheda Modello di minaccia.

Verrai indirizzato alla procedura guidata di configurazione del modello di minaccia, che prevede due passaggi opzionali.

Fase 1: Connect gli archivi del codice sorgente (opzionale)

Connect GitHub i GitLab repository o Bitbucket per i quali desideri abilitare la modellazione delle minacce. I modelli di minaccia stessi vengono creati e visualizzati nell'applicazione web.

> **Important**
>
> Le integrazioni configurate qui sono condivise in tutto il tuo Agent Space. Le modifiche si applicano alla modellazione delle minacce, alla revisione del codice e alle funzionalità di test di penetrazione.

Connect repository

1. Nella sezione Integrazioni connesse, scegli Aggiungi.
2. Seleziona la registrazione che contiene i repository che desideri utilizzare.
3. Seleziona la casella di controllo per ogni repository che desideri connettere.
4. Scegli Salva per applicare le tue selezioni.

> **Note**
>
> Se non hai ancora registrato un'integrazione, scegli Impostazioni per accedere alla pagina Integrazioni in cui puoi autorizzare l'app AWS Security Agent. Per ulteriori informazioni, consulta Connect AWS Security Agent ai GitHub repository, Connect AWS Security Agent ai GitLab repository o Connect AWS Security Agent ai repository Bitbucket.

1. Scegli Avanti per passare alle configurazioni opzionali.

Fase 2: configurazioni opzionali

Configura i bucket S3, la CloudWatch registrazione e le impostazioni di accesso ai servizi per il tuo ambiente di modellazione delle minacce. Queste impostazioni sono condivise con altre funzionalità di Agent Space.

Bucket S3 (opzionali)

Aggiungi bucket S3 contenenti il codice sorgente che desideri che l'agente utilizzi come contesto durante la modellazione delle minacce.

1. Nella sezione bucket S3, scegli Aggiungi risorsa S3.
2. Inserisci l'URI S3 per il bucket o il prefisso.
3. Scegliere Aggiungi.

> **Note**
>
> Puoi aggiungere fino a 10 risorse S3.

CloudWatch registri (facoltativi)

Configura i gruppi di CloudWatch log per acquisire e analizzare il comportamento delle applicazioni durante l'esecuzione del modello di minaccia.

1. Nella sezione CloudWatch log, seleziona uno o più gruppi di CloudWatch log esistenti dal tuo account AWS.

Accesso al servizio

Configura il ruolo del servizio IAM che AWS Security Agent utilizza per accedere alle tue risorse AWS come i bucket S3 e i CloudWatch log per la modellazione delle minacce. È necessario un ruolo di servizio per abilitare la modellazione delle minacce.

1. Nella sezione Accesso al servizio, seleziona un ruolo di servizio IAM esistente dal menu a discesa o lascialo vuoto per creare automaticamente un ruolo di servizio.

> **Note**
>
> Un ruolo di servizio verrà creato automaticamente se non selezioni un ruolo esistente.

1. Scegli Salva per completare la configurazione.

Dopo la configurazione

Dopo aver completato la configurazione della modellazione delle minacce:

- La scheda del modello di minaccia nella pagina Agent Space mostra lo stato Pronto.
- Gli utenti possono avviare l'applicazione Web e creare modelli di minaccia a partire dal codice sorgente connesso, dai documenti scope caricati, dalle pagine Confluence o da una combinazione di questi input.

Fasi successive

Dopo aver abilitato la modellazione delle minacce:

- Avvia l'applicazione web per creare ed eseguire modelli di minaccia (vedi Creare un modello di minaccia)
- Connect repository o bucket S3 aggiuntivi man mano che la tua codebase cresce
- Connect Confluence per abilitare la selezione di pagine come documenti di ambito (vedi Connect AWS Security Agent a Confluence)

Consenti agli utenti di avviare la correzione dei risultati dei test di penetrazione e della revisione del codice

Nella Console di gestione AWS, puoi abilitare la correzione automatica in modo che gli utenti dell'app Web AWS Security Agent possano richiedere correzioni per un risultato specifico. AWS Security Agent fornisce ogni correzione come GitHub pull request sul repository interessato.

Puoi abilitare la riparazione per repository dall'interno di un Agent Space. Le schede Penetration test e Code review aprono la stessa procedura guidata di configurazione del repository, quindi è possibile utilizzare entrambe le schede per gestire l'impostazione di riparazione automatica abilitata. La correzione si applica ai risultati di entrambe le funzionalità, quindi è sufficiente abilitarla una sola volta per repository.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

1. Sono stati abilitati i test di penetrazione (vedithe section called “Abilita il test di penetrazione”) o la revisione del codice (vedi) the section called “Abilita la revisione del codice”
2. Installata e autorizzata l' GitHub app AWS Security Agent per la tua GitHub organizzazione (vedithe section called “Connect AWS Security Agent ai GitHub repository”)

Apri la procedura guidata di configurazione del repository

Scegli il punto di ingresso che corrisponde alla configurazione dei tuoi repository.

Dalla scheda Penetration test

Utilizzate questo percorso per aggiungere GitHub repository per i test di penetrazione e configurare la correzione nello stesso passaggio.

1. Vai alla pagina di panoramica di Agent Space.
2. Scegli la scheda Penetration test.
3. Seleziona una GitHub registrazione proprietaria dei tuoi repository:
   a. Se non hai associato alcuna GitHub registrazione all'Agent Space, scegli Aggiungi nella casella delle informazioni di Connect GitHub to AWS Security Agent per selezionare una registrazione.
   b. Se una o più GitHub registrazioni sono già associate, scegli Aggiungi nella sezione Integrazioni connesse per selezionarne un'altra.

4. Scegli Avanti per scegliere i repository GitHub .
5. Scegli Avanti per configurare le funzionalità del repository.

Dalla scheda Revisione del codice

Usa questo percorso quando i tuoi repository sono già collegati per la revisione del codice.

1. Vai alla pagina di panoramica di Agent Space.
2. Scegli la scheda di revisione del codice.
3. Nella tabella dei GitHub repository, scegli Modifica per aprire la procedura guidata di configurazione del repository.

Abilita la riparazione automatica e salva

Dopo aver raggiunto le funzionalità del repository, segui uno dei percorsi precedenti:

1. Nella colonna Riparazione automatica abilitata, contrassegna ogni repository a cui desideri porre rimedio come Abilitato.
2. Scegli Connect per salvare la configurazione.

Gli utenti dell'app Web possono ora avviare la correzione dei risultati su questi repository e AWS Security Agent aprirà le pull request con le correzioni proposte.

Fornisci risorse agli agenti da un bucket S3

Puoi concedere ad AWS Security Agent l'accesso alle risorse in un bucket S3, come documenti API, documenti sul modello di minaccia e codice sorgente che supporta i test di penetrazione.

Concedi ad AWS Security Agent l'accesso in lettura a un bucket S3 nella Console di gestione AWS. Nell'app web Security Agent, gli utenti selezionano le singole risorse di S3 in base alle esigenze.

1. Vai alla pagina di panoramica di Agent Space
2. Seleziona Azioni, quindi Modifica la configurazione del test di penetrazione
3. Nella sezione S3 bucket, definisci l'URI S3 contenente il bucket S3. Puoi aggiungere più bucket S3.

Abilita un dominio applicativo per i test di penetrazione

Prima di poter eseguire un test di penetrazione su un'applicazione, è necessario aggiungere un dominio di destinazione e verificarne la proprietà. AWS Security Agent eseguirà solo test di penetrazione su domini verificati.

> **Note**
>
> Non è necessario convalidare i domini ausiliari che l'applicazione può utilizzare. Devi solo convalidare il dominio su cui eseguirai attivamente i test di penetrazione.

Fase 1: Aggiungere un dominio di destinazione

Per aggiungere un dominio di destinazione, vai alla scheda Penetration test nella pagina di panoramica di Agent Space. A seconda che il penetration test sia già stato configurato, utilizza uno dei seguenti metodi:

- First-time configurazione: scegli Configura test di penetrazione per aprire la procedura guidata per il test di penetrazione. Nel primo passaggio, inserisci il dominio e scegli un metodo di verifica.
- Aggiungere un dominio a una configurazione esistente: nella tabella Domini di destinazione, scegli Aggiungi dominio. Inserisci il dominio e scegli un metodo di verifica nella modalità modale.

Puoi aggiungere un dominio di base o un sottodominio, ad esempio `example.com` o. `billing.example.com` AWS suggerisce di utilizzare un sottodominio in cui sei autorizzato a creare TXT record.

> **Note**
>
> Quando verifichi un dominio utilizzando la verifica del percorso DNS TXT o HTTP, i sottodomini di quel dominio vengono automaticamente coperti. Ad esempio, la verifica `example.com` consente di eseguire il test `api.example.com` o senza ulteriori verifiche. `billing.example.com` Per la verifica VPC privato, il nome di dominio dell'endpoint di destinazione deve corrispondere al nome di dominio completo configurato per la verifica.

Scegli uno dei seguenti metodi di verifica:

- Record DNS TXT: dimostra la proprietà del dominio creando un record DNS TXT con il tuo provider DNS.
- Percorso HTTP: dimostra la proprietà del dominio creando un percorso sul tuo server Web che contiene un token univoco fornito da AWS Security Agent.
- VPC privato: utilizzabile solo per i test di penetrazione dei VPC privati. Verifica che il dominio si risolva in un IP in un intervallo CIDR privato. Il nome di dominio configurato deve corrispondere al nome di dominio completo di tutti gli endpoint di destinazione associati

Passaggio 2: verifica della proprietà del dominio

Dopo aver aggiunto il dominio, verifica la proprietà utilizzando il metodo selezionato. Puoi attivare la verifica in qualsiasi momento dalla tabella Target Domains selezionando il dominio e scegliendo Verifica.

Verifica utilizzando un record DNS TXT

AWS Security Agent genera un valore di record DNS TXT. Devi aggiungere questo record al tuo provider DNS per dimostrarne la proprietà.

Se il dominio è registrato in Route 53 (stesso account AWS):

AWS Security Agent può creare automaticamente il record DNS. Seleziona il dominio dalla tabella Target Domains e scegli One-click la verifica. AWS Security Agent crea il record di convalida DNS e completa la verifica automaticamente.

Se il dominio è registrato con un altro provider DNS:

1. Copia il valore del record TXT fornito da AWS Security Agent.
2. Aggiungi il record TXT con il tuo registrar DNS.
3. Torna alla tabella Target Domains, seleziona il dominio e scegli Verifica.

Verifica utilizzando la convalida del percorso HTTP

Questo metodo dimostra la proprietà del dominio inserendo un token univoco sul tuo server web. Solo i proprietari di domini o gli amministratori web autorizzati possono creare percorsi su un server Web, il che dimostra la proprietà.

1. Crea un file nel seguente percorso sul tuo server web:

```
.well-known/aws/securityagent-domain-verification.json
```

2. Inserisci il token fornito da AWS Security Agent nel file utilizzando questo formato:

```
{
  "tokens": ["<insert-token>"]
}
```

3. Torna alla tabella Target Domains, seleziona il dominio e scegli Verifica. AWS Security Agent invia una richiesta HTTPS GET all'URL di verifica e convalida il token.
4. Se il dominio è accessibile su Internet pubblico, assicurati che il dominio disponga di un certificato SSL valido prima di eseguire la verifica.

> **Note**
>
> Se il tuo dominio è registrato in più spazi di agenti e utilizzi la convalida del percorso HTTP, puoi inserire i token per entrambi gli spazi degli agenti nello stesso array. `tokens`

Ignora la verifica della proprietà del dominio

I clienti che dispongono dell'autorizzazione a eseguire test di penetrazione su un endpoint ma non possono completare la verifica della proprietà possono richiederci la verifica manuale. Apri una richiesta di assistenza clienti per effettuare questa richiesta. La richiesta deve includere il caso d'uso aziendale e la giustificazione della verifica manuale della proprietà (ad esempio, il motivo per cui sei autorizzato a eseguire test di penetrazione sull'endpoint).

Domini target gestiti utilizzati per i test di penetrazione

Nella Console di gestione AWS, puoi aggiungere e gestire i domini di destinazione utilizzati dagli spazi degli agenti per i test di penetrazione. Questi domini target dovranno essere verificati prima di poter essere utilizzati in un test di penetrazione. Per ulteriori informazioni sulla verifica dei domini di destinazione, consulta the section called “Abilita il test di penetrazione”

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

1. Test di penetrazione abilitato (vedi) the section called "Abilita il test di penetrazione"

Gestisci le risorse del dominio di destinazione

- Vai alla pagina di panoramica dei domini di Target.
- Dovresti vedere tutte le risorse del dominio di destinazione associate al tuo account
  - Se non vedi alcun dominio di destinazione associato al tuo account, segui i passaggi indicati the section called "Abilita il test di penetrazione" per creare e verificare un dominio di destinazione
- I domini di destinazione possono essere riutilizzati tra gli spazi degli agenti e condividere lo stato di verifica
  - Per aggiungere un dominio di destinazione esistente a uno spazio agente, vai alla scheda Penetration test dello spazio agente. Seleziona Aggiungi dominio e scegli il dominio desiderato in Seleziona tra i domini precedentemente registrati disponibili nel campo del nome di dominio
  - I domini di destinazione devono essere associati a uno spazio agente prima di poter essere utilizzati in un test di penetrazione
- La rimozione di un dominio da uno spazio agente non elimina il dominio. Il dominio di destinazione associato può essere eliminato definitivamente dalla pagina di panoramica di Target Domains

Verifica i domini di destinazione

Affinché un dominio di destinazione possa essere utilizzato in un test di penetrazione, deve prima essere verificato utilizzando uno dei seguenti metodi:

- Domini Route 53 (stesso account AWS): scegli One-click la verifica. AWS Security Agent crea automaticamente il record DNS e completa la verifica.
- DNS TXT (altri provider DNS): copia il token di verifica, aggiungi il record TXT con il tuo registrar DNS, quindi seleziona il dominio e scegli Verifica.
- Percorso HTTP: posiziona il token di verifica sul percorso di percorso richiesto sul tuo server web, quindi seleziona il dominio e scegli Verifica. Per informazioni dettagliate, vedi the section called "Abilita un dominio applicativo per i test di penetrazione".
- VPC privato: verifica che l'IP del dominio di destinazione rientri in un intervallo CIDR privato (vedi the section called "Connect agent a risorse VPC private" per un elenco di intervalli CIDR privati). Il nome di dominio dell'endpoint di destinazione del test di penetrazione deve corrispondere al nome di dominio completo configurato per la verifica. Utilizzabile solo per test di penetrazione di VPC privati

> **Note**
>
> Per la verifica DNS TXT, HTTP route e Route 53, i sottodomini di un dominio verificato sono automaticamente coperti e non richiedono una verifica separata. Per la verifica tramite VPC privato, ogni dominio deve essere verificato singolarmente.

Gestione dei requisiti di sicurezza

Definisci i requisiti di sicurezza che AWS Security Agent valuta durante la progettazione e le revisioni del codice, utilizzando AWS-managed pacchetti, pacchetti personalizzati o requisiti importati dalla tua documentazione.

Gestisci i requisiti di sicurezza

Organizza i requisiti di sicurezza utilizzati da AWS Security Agent per analizzare le tue applicazioni in pacchetti di requisiti di sicurezza. Un pacchetto è una raccolta di requisiti di sicurezza. Puoi abilitare AWS-managed pack, creare pacchetti personalizzati e generare requisiti per un pacchetto personalizzato caricando la documentazione di sicurezza.

Panoramica di

Un requisito di sicurezza definisce uno standard o una politica di sicurezza in base al quale AWS Security Agent valuta l'applicazione durante le revisioni del progetto e le revisioni del codice. Quando un progetto o un codice non soddisfano un requisito, AWS Security Agent segnala un risultato. Ogni requisito di sicurezza appartiene a un pacchetto di requisiti di sicurezza. I requisiti di sicurezza sono condivisi tra tutti gli Agent Spaces e valutati durante la progettazione e le revisioni del codice.

AWS Security Agent fornisce due tipi di pacchetti, mostrati in schede separate:

- Pacchetti di requisiti di sicurezza gestiti: pacchetti di requisiti di sicurezza AWS forniti in base agli standard e alle migliori pratiche del settore. È possibile abilitare istantaneamente questi pacchetti per effettuare valutazioni in base alle politiche di sicurezza più comuni senza configurazioni personalizzate. I requisiti di un pacchetto gestito sono di sola lettura. È possibile utilizzare un AWS requisito gestito come modello per un requisito personalizzato. Per l'elenco dei pacchetti gestiti disponibili, consulta i pacchetti di requisiti di sicurezza AWS gestiti.
- Pacchetti di requisiti di sicurezza personalizzati: pacchetti creati per applicare le politiche e gli standard specifici dell'organizzazione. Puoi creare i requisiti in un pacchetto personalizzato

partendo da zero, personalizzando i requisiti AWS gestiti come punto di partenza o generandoli caricando la documentazione di sicurezza.

> **Note**
>
> I pacchetti di framework di conformità sono progettati per aiutare a identificare i requisiti di sicurezza che possono essere rilevanti per la conformità a determinati framework. Non valutano la vostra conformità né garantiscono il superamento di un audit.

I pacchetti vengono abilitati e disattivati come unità. Quando un pacchetto è abilitato, AWS Security Agent valuta le applicazioni in base ai requisiti del pacchetto durante la progettazione e le revisioni del codice.

> **Note**
>
> L'attivazione o la disabilitazione di un pacchetto si applica alle nuove revisioni dei progetti e alle revisioni del codice. Le recensioni esistenti non sono interessate.

Abilita o disabilita un pacchetto gestito

Abilita un pacchetto AWS-managed per valutare le tue applicazioni rispetto a una serie di requisiti AWS di sicurezza mantenuti. Disattivalo quando non ti serve più.

1. Nella AWS console, accedi a AWS Security Agent.
2. Nel riquadro di navigazione, scegli Requisiti di sicurezza.
3. Scegli la scheda Pacchetti di requisiti di sicurezza gestiti.
4. Seleziona il pacchetto che desideri abilitare o disabilitare.
5. Esegui una delle seguenti operazioni:
   a. Per abilitare il pacchetto, scegli Abilita pacchetto.
   b. Per disabilitare il pacchetto, scegli Disabilita pacchetto.

> **Tip**
>
> Scegli un pacchetto per visualizzare i requisiti di sicurezza che contiene. Scegli un requisito per visualizzarne la definizione completa, compresa l'applicabilità, i criteri di conformità e le linee guida per la correzione.

Crea un pacchetto personalizzato

Crea un pacchetto personalizzato per raggruppare i requisiti di sicurezza specifici della tua organizzazione. Dopo aver creato il pacchetto, aggiungi i requisiti manualmente, personalizza un requisito AWS gestito o carica i documenti per generare i requisiti.

1. Nella AWS console, accedi a AWS Security Agent.
2. Nel riquadro di navigazione, scegli Requisiti di sicurezza.
3. Scegli la scheda Pacchetti di requisiti di sicurezza personalizzati.
4. Scegli Crea pacchetto di requisiti di sicurezza.
5. Inserisci il nome del pacchetto dei requisiti di sicurezza e una descrizione opzionale.
6. Scegli Crea pacchetto di requisiti di sicurezza.

> **Note**
>
> Dopo aver creato un pacchetto, puoi aggiungere o caricare documenti sorgente per generare i requisiti di sicurezza per il pacchetto.

Aggiungi manualmente un requisito di sicurezza

Aggiungi un requisito di sicurezza a un pacchetto personalizzato per definire uno standard di sicurezza applicato da AWS Security Agent.

1. Nella AWS console, accedi a AWS Security Agent.
2. Nel riquadro di navigazione, scegli Requisiti di sicurezza.
3. Scegli la scheda Pacchetti di requisiti di sicurezza personalizzati, quindi scegli il pacchetto a cui desideri aggiungere un requisito.
4. Scegli Aggiungi requisito manualmente.

5. Configura i campi seguenti:
   a. Nome del requisito di sicurezza: inserisci un nome descrittivo che identifichi il controllo di sicurezza, ad esempio `enforce-encryption-at-rest` (massimo 80 caratteri).
   b. Descrizione: fornisci una breve descrizione di ciò che controlla questo requisito di sicurezza (massimo 500 caratteri).
   c. Applicabilità: descrivi gli scenari, i tipi di sistema o le condizioni in cui questo requisito di sicurezza deve essere valutato. Includi gli scenari in cui il requisito deve essere contrassegnato come NOT_APPLICABLE (massimo 10.000 caratteri).
   d. Criteri di conformità: definisci cosa costituisce conformità e non conformità per questo requisito di sicurezza. Fornisci gli indicatori, gli esempi e i dettagli tecnici che AWS Security Agent cerca quando valuta la conformità (massimo 10.000 caratteri).
   e. Guida alla correzione (facoltativa): fornisci indicazioni su come correggere le violazioni, inclusi collegamenti alla documentazione o agli standard interni dell'organizzazione (massimo 10.000 caratteri).
6. Esegui una delle seguenti operazioni:
   a. Per creare il requisito senza abilitarlo, scegli Crea requisito di sicurezza.
   b. Per creare il requisito e abilitarlo, scegli Crea e abilita il requisito di sicurezza.

> **Note**
>
> Un requisito viene valutato durante le revisioni di sicurezza solo quando il pacchetto che lo contiene è abilitato. Per controllare se un pacchetto viene valutato, abilita o disabilita il pacchetto.

Personalizza un AWS-requisito di sicurezza gestito

Crea un requisito di sicurezza personalizzato che utilizzi un requisito AWS gestito come punto di partenza. AWS Security Agent precompila i dettagli dei requisiti dal requisito gestito e li modifica per adattarli alla tua organizzazione.

1. Nella AWS console, accedi a AWS Security Agent.
2. Nel riquadro di navigazione, scegli Requisiti di sicurezza.
3. Scegli la scheda Pacchetti di requisiti di sicurezza personalizzati, quindi scegli il pacchetto personalizzato a cui aggiungere il requisito.

4. Scegli Crea requisito di sicurezza personalizzato.
5. Per precompilare il modulo, nella sezione Personalizza un requisito di sicurezza AWS gestito, cerca e seleziona un requisito AWS gestito da utilizzare come modello.
6. Modifica qualsiasi campo per adattarlo alle esigenze della tua organizzazione.
7. Esegui una delle seguenti operazioni:
   a. Per creare il requisito senza abilitarlo, scegli Crea requisito di sicurezza.
   b. Per creare e abilitare immediatamente il requisito, scegli Crea e abilita il requisito di sicurezza.

> **Note**
>
> La personalizzazione di un requisito AWS gestito crea un requisito di sicurezza personalizzato indipendente. Le modifiche successive al requisito AWS-managed non influiscono sulla versione personalizzata.

Genera i requisiti caricando i documenti

Genera i requisiti di sicurezza per un pacchetto personalizzato dalla documentazione di sicurezza esistente invece di scrivere ogni requisito a mano. AWS Security Agent legge i documenti caricati, identifica i contenuti rilevanti per la sicurezza e genera requisiti strutturati che puoi rivedere e modificare. Per la procedura completa, consulta Generazione dei requisiti di sicurezza dai documenti. Per indicazioni su cosa includere nei documenti caricati, consulta Preparare i documenti per la generazione dei requisiti.

> **Important**
>
> Il caricamento di nuovi documenti sorgente rigenera tutti i requisiti del pacchetto. Tutti i requisiti esistenti, inclusi quelli aggiunti manualmente, vengono sostituiti.

Modifica un requisito di sicurezza personalizzato

Modifica un requisito di sicurezza personalizzato per aggiornarne la definizione, i criteri o le linee guida per la correzione. Non è possibile modificare i requisiti in un AWS-managed pack.

1. Nella AWS console, accedi a AWS Security Agent.

2. Nel riquadro di navigazione, scegli Requisiti di sicurezza.
3. Scegli la scheda Pacchetti di requisiti di sicurezza personalizzati, quindi scegli il pacchetto che contiene il requisito.
4. Seleziona il requisito che desideri modificare, quindi scegli Modifica requisito di sicurezza personalizzato.
5. Aggiorna i campi dei requisiti secondo necessità. Il nome del requisito di sicurezza non può essere modificato dopo la creazione.
6. Scegli Aggiorna requisito di sicurezza.

> **Note**
>
> Le modifiche a un requisito di sicurezza si applicano alle nuove revisioni progettuali e alle revisioni del codice. Le recensioni esistenti non sono interessate.

Abilita o disabilita un pacchetto

Abilita o disabilita un pacchetto di requisiti di sicurezza per controllare se AWS Security Agent valuta i requisiti in esso contenuti. I pacchetti vengono attivati e disattivati come unità.

1. Nella AWS console, accedi a AWS Security Agent.
2. Nel riquadro di navigazione, scegli Requisiti di sicurezza.
3. Scegli la scheda relativa al tipo di pacchetto, quindi seleziona il pacchetto.
4. Esegui una delle seguenti operazioni:
   a. Per abilitare il pacchetto, scegli Abilita pacchetto.
   b. Per disabilitare il pacchetto, scegli Disabilita pacchetto.

> **Note**
>
> Quando un pacchetto è abilitato, i requisiti del pacchetto vengono valutati durante le revisioni di sicurezza. Quando un pacchetto è disabilitato, i relativi requisiti non vengono valutati.

Eliminare un requisito di sicurezza personalizzato

Eliminare un requisito di sicurezza personalizzato quando non si desidera più che AWS Security Agent lo valuti.

1. Nella AWS console, accedi a AWS Security Agent.
2. Nel riquadro di navigazione, scegli Requisiti di sicurezza.
3. Scegli la scheda Pacchetti di requisiti di sicurezza personalizzati, quindi scegli il pacchetto che contiene il requisito.
4. Seleziona uno o più requisiti di sicurezza, quindi scegli Elimina requisito di sicurezza.
5. Conferma l'eliminazione.

> **Note**
>
> Quando elimini i requisiti di sicurezza, questi non vengono più valutati nelle revisioni future. I requisiti rimangono visibili nelle revisioni precedenti come risultati di sola lettura.

Le migliori pratiche per definire i requisiti di sicurezza

Quando crei un requisito di sicurezza, segui queste linee guida per aiutare AWS Security Agent a valutare le tue applicazioni in modo accurato e fornire risultati utilizzabili.

Nome del requisito di sicurezza: utilizza un nome chiaro e specifico che identifichi il controllo di sicurezza. Evita termini generici che non descrivono lo scopo del requisito.

Descrizione: spiega cosa controlla il controllo e il rischio che mitiga. Questo aiuta gli utenti a capire perché il requisito è importante.

Applicabilità: descrivi i carichi di lavoro, i tipi di sistema o le condizioni in cui è necessario valutare il requisito. Indica quando il requisito deve essere contrassegnato come NOT_APPLICABILE, con scenari specifici, per evitare falsi positivi. Frasi come «Questo controllo si applica a TUTTI i carichi di lavoro che...» e «Contrassegna come NOT_APPLICABLE if...» definiscono limiti chiari dell'ambito.

Criteri di conformità: strutturali in due parti: cosa dimostra la conformità e cosa indica la non conformità. Sii specifico con gli indicatori tecnici e includi i casi limite. Inizia con «Un design è conforme se dimostra...» seguito dai dettagli tecnici, quindi «Un design è non conforme se...» con gli schemi che indicano una violazione.

Guida alla riparazione: fornisce indicazioni con dettagli tecnici ed esempi di configurazione. Includi link alla documentazione interna della tua organizzazione in modo che gli sviluppatori abbiano a disposizione le risorse necessarie per correggere le violazioni.

Fasi successive

Dopo aver configurato i pacchetti dei requisiti di sicurezza:

- Crea una revisione del progetto o una revisione del codice per valutare la tua applicazione rispetto ai pacchetti che hai abilitato.
- Attiva i test di penetrazione per integrare le tue revisioni di progettazione e codice.
- Concedi agli utenti l'accesso all'app web AWS Security Agent.

Pacchetti di requisiti di sicurezza gestiti da AWS

Un pacchetto di requisiti di sicurezza AWS gestiti è una raccolta di requisiti di sicurezza che AWS crea e mantiene, in base agli standard e alle migliori pratiche del settore. È possibile consentire a un pacchetto gestito di valutare le applicazioni rispetto ai relativi requisiti durante le revisioni della progettazione e le revisioni del codice, senza dover scrivere personalmente i requisiti.

I requisiti di sicurezza in un pacchetto gestito sono di sola lettura. Non è possibile modificarli. È possibile utilizzare un requisito AWS gestito come modello per creare un requisito personalizzato e quindi modificare la copia per adattarla alla propria organizzazione. Per ulteriori informazioni, consulta Gestire i requisiti di sicurezza.

AWS aggiorna i pacchetti gestiti nel tempo. Quando AWS aggiunge o modifica un requisito in un managed pack, la modifica si applica a tutti gli account che hanno il pacchetto abilitato.

> **Note**
>
> I pacchetti del framework di conformità sono progettati per aiutare a identificare i requisiti di sicurezza che possono essere rilevanti per la conformità a determinati framework. Non valutano la vostra conformità né garantiscono il superamento di un audit.

Pacchetto gestito AWS: ASA Base Pack

Una serie di requisiti di sicurezza di base che si applicano alla maggior parte dei carichi di lavoro. Questo pacchetto copre problemi comuni di sicurezza delle applicazioni come l'autenticazione

e l'autorizzazione, la protezione dei dati, la registrazione e la convalida degli input. Attiva questo pacchetto per stabilire una base di sicurezza per la progettazione e le revisioni del codice.

Pacchetto gestito AWS: AWS Well-Architected Pack

Requisiti di sicurezza derivati dal pilastro della sicurezza del AWS Well-Architected Framework. Questo pacchetto valuta l'applicazione in base AWS alle indicazioni per la protezione dei dati, la gestione di identità e autorizzazioni e il rilevamento e la risposta agli eventi di sicurezza. Per ulteriori informazioni sul framework, consulta Security Pillar - AWS Well-Architected Framework.

Pacchetto gestito AWS: NIST CSF Pack

Requisiti di sicurezza derivati dal NIST Cybersecurity Framework (CSF). Questo pacchetto valuta l'applicazione rispetto alle aree di controllo tratte dal framework, come la gestione delle identità e degli accessi, la sicurezza dei dati e la tecnologia di protezione. Abilita questo pacchetto per allineare le revisioni del design e del codice con NIST CSF.

Pacchetto gestito AWS: pacchetto PCI DSS

Requisiti di sicurezza derivati dal Payment Card Industry Data Security Standard (PCI DSS). Questo pacchetto valuta l'applicazione rispetto alle aree di controllo relative alla gestione dei dati dei titolari di carta, come il controllo degli accessi, la crittografia dei dati in transito e in archivio e la registrazione. Attiva questo pacchetto per allineare la progettazione e le revisioni del codice con PCI DSS.

Genera requisiti di sicurezza dai documenti

Genera i requisiti di sicurezza per un pacchetto personalizzato caricando la documentazione di sicurezza esistente. AWS Security Agent legge i documenti caricati, identifica i contenuti rilevanti per la sicurezza e genera requisiti di sicurezza strutturati con criteri di applicabilità, conformità e linee guida per la correzione. È possibile esaminare e modificare i requisiti generati prima che vengano utilizzati nelle revisioni.

Utilizzatelo invece di scrivere ogni requisito a mano quando avete già documentato le politiche, gli standard o le linee guida di sicurezza. Per indicazioni su cosa includere nei documenti che carichi, consulta Preparare i documenti per la generazione dei requisiti.

Formati file supportati

Puoi caricare i seguenti formati di file:

- DOC
- DOCX
- MD
- PDF
- TXT

Genera requisiti

1. Nella AWS console, accedi a AWS Security Agent.
2. Nel riquadro di navigazione, scegli Requisiti di sicurezza.
3. Scegli la scheda Pacchetti di requisiti di sicurezza personalizzati.
4. Crea un pacchetto o scegli un pacchetto personalizzato esistente per cui generare i requisiti.
5. Scegli i file o trascina i documenti nell'area di caricamento.
6. Scegli Genera requisiti.
7. Attendi che AWS Security Agent elabori i documenti. La generazione viene eseguita in background e può richiedere un paio di minuti per file di grandi dimensioni. Non è possibile avviare un altro caricamento del pacchetto mentre la generazione è in corso.
8. Rivedi i requisiti di sicurezza generati. Modifica, elimina o aggiungi i requisiti secondo necessità. Attiva il pacchetto quando desideri che AWS Security Agent ne valuti i requisiti durante le revisioni di sicurezza.

> **Note**
>
> AWS Security Agent genera requisiti a livello di carico di lavoro e si concentra sui contenuti rilevanti per la sicurezza nei documenti. Il numero di requisiti che genera dipende dal contenuto fornito. Controlla i requisiti generati per confermare che riflettano le tue intenzioni.

Sostituisci i requisiti con un nuovo caricamento

Il caricamento di nuovi documenti sorgente rigenera i requisiti per un pacchetto.

> **Important**
>
> Quando si caricano nuovi documenti sorgente in un pacchetto, AWS Security Agent rigenera tutti i requisiti per quel pacchetto. Tutti i requisiti esistenti, inclusi quelli aggiunti manualmente, vengono sostituiti. Per mantenere i requisiti attuali, non caricare nuovi documenti.

1. Nella AWS console, accedi a AWS Security Agent.
2. Nel riquadro di navigazione, scegli Requisiti di sicurezza.
3. Scegli la scheda Pacchetti di requisiti di sicurezza personalizzati, quindi scegli il pacchetto.
4. Inizia un nuovo caricamento e conferma che il caricamento di nuovi documenti sorgente sostituisce i requisiti esistenti.
5. Scegli i tuoi file, quindi scegli Genera requisiti.

Fasi successive

- Rivedi e abilita i requisiti generati. Vedi Gestire i requisiti di sicurezza.
- Crea una revisione del progetto o una revisione del codice per valutare la tua applicazione rispetto al pacchetto.

Preparare i documenti per la generazione dei requisiti

Quando si generano requisiti di sicurezza dai documenti, AWS Security Agent legge i documenti e produce requisiti strutturati sulla base dei contenuti rilevanti per la sicurezza che trova. Non è necessario formattare i documenti in alcun modo particolare o prescrivere l'applicabilità, i criteri di conformità e le linee guida per la correzione. AWS Security Agent li ricava dai contenuti forniti dall'utente. Carica la documentazione di sicurezza che già possiedi, scritta con parole tue.

Questa pagina descrive cosa includere in modo che AWS Security Agent generi requisiti accurati e utili. Per la procedura di caricamento e i limiti dei file, vedere Generazione dei requisiti di sicurezza dai documenti.

Cosa includere

AWS Security Agent cerca contenuti che descrivano le tue aspettative di sicurezza. I documenti che trattano i seguenti argomenti producono i requisiti più rigorosi:

- Controllo e autorizzazione degli accessi
- Autenticazione
- Protezione e crittografia dei dati
- Sicurezza di rete
- Registrazione e controllo
- Risposta agli incidenti
- Gestione delle vulnerabilità e delle patch
- Obblighi di conformità che si applicano ai carichi di lavoro

I buoni documenti di origine includono politiche di sicurezza, standard tecnici, cataloghi di controllo, linee guida sull'architettura e standard di codifica sicuri.

Scrivi a livello di carico di lavoro

AWS Security Agent genera requisiti che si applicano a un singolo carico di lavoro o applicazione, lo stesso ambito che valuta durante la progettazione e le revisioni del codice. I contenuti che descrivono come creare e gestire un carico di lavoro sicuro generano requisiti. Organization-wide gli argomenti di governance, come la strategia multi-account, la gestione degli utenti root e la configurazione della registrazione a livello di account, non rientrano in questo ambito e non generano requisiti di carico di lavoro.

Descrivi il risultato, non una singola implementazione

Indica il risultato di sicurezza che ti aspetti anziché un singolo prodotto o configurazione prescritti. AWS Security Agent genera requisiti incentrati sulla funzionalità di sicurezza necessaria e consentono più di un'implementazione valida. Ad esempio, «i dati inattivi sono crittografati» genera un requisito più chiaro e più ampiamente applicabile rispetto a un'istruzione che nomina un servizio o un'impostazione specifici.

Sii specifico su cosa significhi essere bello

Quanto più concretamente i documenti descrivono il comportamento previsto, tanto meglio AWS Security Agent è in grado di definire i criteri di conformità. Se possibile, descrivete cosa dimostra un design conforme e cosa indica una violazione. Le affermazioni vaghe o puramente ambiziose generano un numero inferiore di requisiti e sono più deboli rispetto a quelle concrete e pertinenti al carico di lavoro.

Controlla cosa ottieni in cambio

Ogni requisito generato include un nome, l'applicabilità, i criteri di conformità e le linee guida per la correzione che AWS Security Agent ha tratto dai tuoi documenti. Rivedi i requisiti generati, modifica quelli che necessitano di perfezionamento e abilita quelli che desideri che AWS Security Agent valuti. Per ulteriori informazioni, consulta Gestire i requisiti di sicurezza.

Gestione degli utenti e degli accessi

Controlla chi può accedere a ogni Agent Space e configura i ruoli IAM e le chiavi di crittografia utilizzate da AWS Security Agent.

Concedi agli utenti l'accesso all'app Web AWS Security Agent

AWS Security Agent offre agli utenti due metodi per accedere all'applicazione Web, a seconda di come hai configurato l'Agent Space durante la configurazione.

Panoramica dei metodi di accesso

IAM Identity Center (SSO): se hai abilitato IAM Identity Center durante la creazione del tuo Agent Space, gli utenti possono accedere all'applicazione web direttamente tramite SSO. Assegni gli utenti all'Agent Space tramite la console AWS Security Agent e gli utenti accedono utilizzando le loro credenziali Identity Center.

Accesso da amministratore: gli utenti con accesso alla console AWS possono avviare l'applicazione Web tramite un link di accesso amministratore nella pagina di panoramica di Agent Space nella Console di gestione AWS.

Concedi l'accesso con IAM Identity Center (SSO)

Se hai configurato il tuo Agent Space con IAM Identity Center, puoi assegnare utenti all'Agent Space utilizzando la console AWS Security Agent.

Assegna utenti tramite la console AWS Security Agent

1. Nella Console di gestione di AWS Security Agent, accedi al tuo Agent Space.
2. Seleziona la scheda dell'app Web.
3. Nella tabella Utenti, scegli Aggiungi utenti.

4. Seleziona gli utenti esistenti da IAM Identity Center o crea nuovi utenti.
5. Conferma le assegnazioni degli utenti.

> **Tip**
>
> Gli utenti assegnati all'Agent Space possono accedere all'applicazione web accedendo tramite IAM Identity Center con le proprie credenziali SSO.

Accedi all'applicazione web con SSO

Dopo l'assegnazione degli utenti all'Agent Space:

1. Gli utenti accedono all'URL dell'applicazione Web per Agent Space.

   > **Tip**
   >
   > Trova l'URL dell'app Web nella pagina dei dettagli di Agent Space nella console AWS Security Agent selezionando Copia l'URL dell'app web. Gli utenti devono aggiungere questo URL ai preferiti per un facile accesso.

2. Gli utenti accedono utilizzando le proprie credenziali SSO.
3. Dopo l'autenticazione, gli utenti possono selezionare Agent Space e iniziare a condurre valutazioni di sicurezza.

Concedi l'accesso con accesso IAM-only

Se hai configurato Agent Space con IAM-only access, gli utenti con accesso alla console AWS possono avviare l'applicazione Web tramite un link di accesso da amministratore.

Usa il link di accesso all'amministratore

1. Accedi alla console AWS Security Agent.
2. Accedi all'Agent Space a cui desideri accedere.
3. Nella scheda dell'app Web della pagina di destinazione di Agent Space, scegli il pulsante di accesso come amministratore per avviare l'applicazione Web.
4. L'applicazione Web si apre in una nuova scheda con l'utente autenticato automaticamente.

> **Note**
>
> Il link di accesso all'amministratore è disponibile solo per gli utenti che sono già autenticati alla Console AWS con le autorizzazioni AWS Security Agent appropriate. Questo metodo non richiede la configurazione di IAM Identity Center.

Fasi successive

Dopo aver concesso agli utenti l'accesso all'applicazione web:

- Gli utenti possono creare e gestire configurazioni ed esecuzioni di test di penetrazione
- Gli utenti possono creare e gestire le revisioni dei progetti
- Gli utenti possono visualizzare i risultati di sicurezza e le linee guida per la correzione
- Configura le preferenze di notifica per i risultati di sicurezza

Crea un ruolo IAM per AWS Security Agent

AWS Security Agent utilizza IAM Roles in tre modi:

1. Ruolo dell'applicazione: utilizzato durante la creazione dell'applicazione AWS Security Agent. Per i casi d'uso di IAM Identity Center e Admin Access Link, il servizio assume questo ruolo per concedere WebApp agli utenti le autorizzazioni per interagire con le API di AWS Security Agent.
2. Ruolo del servizio Penetration Test: specificato durante la creazione di spazi per agenti come elenco di ruoli disponibili. Successivamente, WebApp gli utenti selezionano uno di questi ruoli durante la creazione di un test di penetrazione. Il servizio AWS Security Agent assume questo ruolo per accedere alle risorse AWS durante i test.
3. Ruolo dell'attore: utilizzato per autenticare e autorizzare le richieste all'applicazione Web di destinazione (ad esempio, le API AWS API Gateway). Questi ruoli vengono forniti durante la creazione dello spazio degli agenti. L'agente AWS Security Agent assume i ruoli di attore per interagire con l'applicazione di destinazione.

Ruolo dell'applicazione

L'Application Role viene utilizzato durante la creazione dell'applicazione AWS Security Agent nel servizio. Per gli scenari di autenticazione di IAM Identity Center e Admin Access Link, il servizio AWS

Security Agent assume questo ruolo per concedere WebApp agli utenti le autorizzazioni necessarie per interagire con le API di AWS Security Agent.

Autorizzazioni richieste

Questo ruolo richiede le autorizzazioni per:

- Richiama le operazioni API di AWS Security Agent
- Leggi e scrivi i dati di configurazione delle applicazioni
- Accedere alle informazioni sulla sessione utente
- Gestisci i token di autenticazione per gli utenti WebApp

Policy di attendibilità

La policy di fiducia deve consentire al servizio AWS Security Agent di assumere questo ruolo:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Policy di autorizzazione

Il ruolo deve includere le autorizzazioni per:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "securityagent:GetApplication",
        "securityagent:UpdateApplication",
```

```
        "securityagent:ListAgentInstances",
        "securityagent:CreatePentestSession"
      ],
      "Resource": "arn:aws:securityagent:*:*:application/*"
    }
  ]
}
```

> **Note**
>
> Personalizza le autorizzazioni in base ai requisiti specifici dell'applicazione e al principio del privilegio minimo.

Ruolo del servizio Penetration Test

Il ruolo del servizio Penetration Test viene specificato durante la creazione degli spazi degli agenti come elenco di ruoli disponibili. Quando WebApp gli utenti creano un penetration test, selezionano uno di questi ruoli. Il servizio AWS Security Agent assume quindi questo ruolo per accedere e testare le tue risorse AWS.

Autorizzazioni richieste

Questo ruolo richiede le autorizzazioni per accedere e analizzare le risorse AWS durante i test di penetrazione:

- Leggi e descrivi le configurazioni VPC e la topologia di rete
- Ispeziona le istanze EC2, i gruppi di sicurezza e gli ACL di rete
- Analizza le politiche IAM e le autorizzazioni delle risorse
- Leggi i CloudWatch log e le metriche
- Accedi alle configurazioni dei servizi AWS pertinenti ai test di sicurezza

Policy di attendibilità

La policy di fiducia deve consentire al servizio AWS Security Agent di assumere questo ruolo per le operazioni di test di penetrazione:

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "your-external-id"
        }
      }
    }
  ]
}
```

> **Note**
>
> Usa un ID esterno per una maggiore sicurezza quando consenti l'accesso a più account o servizi.

Policy di autorizzazione

Il ruolo dovrebbe includere l'accesso in sola lettura alle risorse AWS. Prendi in considerazione l'utilizzo di queste politiche gestite:

- `SecurityAudit`- Policy gestita da AWS per il controllo della sicurezza
- `ViewOnlyAccess`- Read-only accesso alla maggior parte dei servizi AWS

Oppure crea una policy personalizzata con autorizzazioni specifiche:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:Describe*",
        "vpc:Describe*",
```

```
        "iam:Get*",
        "iam:List*",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Important**
>
> Concedi solo le autorizzazioni minime richieste per l'ambito dei test di penetrazione. Rivedi e modifica le autorizzazioni in base ai servizi AWS che desideri includere nei test di sicurezza.

Ruolo dell'attore

Il ruolo dell'attore viene utilizzato per autenticare e autorizzare le richieste all'applicazione web di destinazione durante i test di penetrazione. Questi ruoli vengono forniti durante la creazione dello spazio dell'agente e l'agente AWS Security Agent li assume per interagire con gli endpoint dell'applicazione di destinazione (come le API AWS API Gateway, gli URL delle funzioni Lambda o altre applicazioni). AWS-hosted

Autorizzazioni richieste

Questo ruolo richiede le autorizzazioni per:

- Richiama gli endpoint API Gateway
- Esegui funzioni Lambda
- Accedi a risorse AWS specifiche per le applicazioni
- Effettua l'autenticazione con i meccanismi di autenticazione dell'applicazione di destinazione
- Esegui operazioni HTTP sugli endpoint dell'applicazione

Policy di attendibilità

La policy di fiducia deve consentire al servizio AWS Security Agent di assumere questo ruolo:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "your-external-id"
        }
      }
    }
  ]
}
```

Policy di autorizzazione

Le autorizzazioni dipendono dall'architettura dell'applicazione di destinazione. Ecco alcuni esempi di scenari comuni:

Per applicazioni API Gateway

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "execute-api:Invoke"
      ],
      "Resource": "arn:aws:execute-api:us-east-1:*:your-api-id/*"
    }
  ]
}
```

Per gli URL delle funzioni Lambda

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lambda:InvokeFunctionUrl",
        "lambda:InvokeFunction"
      ],
      "Resource": "arn:aws:lambda:us-east-1:*:function:your-function-name"
    }
  ]
}
```

Per Application Load Balancer con autenticazione Cognito

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cognito-idp:InitiateAuth",
        "cognito-idp:RespondToAuthChallenge"
      ],
      "Resource": "arn:aws:cognito-idp:us-east-1:*:userpool/your-user-pool-id"
    }
  ]
}
```

Important

Configura le autorizzazioni Actor Role in modo che soddisfino i requisiti di autenticazione e autorizzazione dell'applicazione di destinazione. Il ruolo deve avere lo stesso livello di accesso degli utenti o dei servizi che il Security Agent simulerà durante i test di penetrazione.

Chiavi gestite dal cliente per AWS Security Agent

Per impostazione predefinita, AWS Security Agent crittografa tutti i dati inattivi utilizzando chiavi AWS di crittografia gestite. Facoltativamente, puoi utilizzare una chiave gestita dal cliente del AWS Key Management Service (AWS KMS) per crittografare i tuoi dati, ottenendo il pieno controllo sulle chiavi di crittografia che proteggono le tue risorse.

AWS Security Agent supporta chiavi gestite dal cliente a livello di risorsa. Quando si crea una risorsa di primo livello come un Agent Space o un'integrazione, è possibile specificare una chiave KMS per crittografare tutti i dati appartenenti a quella risorsa e alle relative sottorisorse. Ad esempio, se si specifica una chiave gestita dal cliente durante la creazione di un Agent Space, vengono crittografati tutti i dati associati a tale Agent Space, incluse le configurazioni di Agent Space, le configurazioni dei test di penetrazione, i processi e i dettagli di esecuzione, i risultati di sicurezza, gli endpoint rilevati e gli screenshot. Puoi anche fornire AWS risorse già crittografate con la tua chiave gestita dal cliente, come i bucket S3, i gruppi di log CloudWatch Logs o i segreti di Secrets Manager. Per le autorizzazioni KMS richieste, consulta. the section called “Autorizzazioni KMS richieste”

Come funzionano le chiavi gestite dai clienti

AWS Security Agent utilizza il portachiavi gerarchico AWS KMS per crittografare i dati con chiavi gestite dal cliente. Quando specifichi una chiave KMS durante la creazione di risorse, il servizio crea una chiave branch protetta dalla tua chiave KMS e la archivia in un Amazon DynamoDB-based key store. Per ogni operazione di crittografia, il portachiavi Hierarchical ricava una chiave di wrapping unica dalla chiave branch attiva, che crittografa una chiave di crittografia dei dati unica per ogni richiesta.

Il portachiavi Hierarchical offre i seguenti vantaggi:

- Per-resource ambito di crittografia: ogni risorsa di primo livello ha la propria chiave di filiale, quindi i dati relativi a risorse diverse vengono crittografati con chiavi separate.
- Rotazione automatica delle chiavi: AWS Security Agent ruota periodicamente le chiavi di filiale. Dopo la rotazione, i nuovi dati vengono crittografati con la nuova versione della chiave branch, mentre le versioni precedenti vengono conservate per decrittografare i dati precedentemente crittografati.

Contesto di crittografia

AWS Security Agent utilizza il contesto di crittografia in tutte le operazioni crittografiche con la chiave KMS. Il contesto di crittografia è un insieme di coppie chiave-valore non segrete che fornisce dati autenticati aggiuntivi per l'operazione di crittografia.

La chiave del contesto di crittografia segue il formato`aws:securityagent:_<resource-type>_`, dove *`<resource-type>`* è il tipo di risorsa da crittografare (ad esempio, o). `agent-space` `integration` Il valore è l'Amazon Resource Name (ARN) della risorsa.

> **Note**
>
> Per le integrazioni, la chiave di contesto di crittografia include il `aws-crypto-ec:` prefisso, che determina il formato. `aws-crypto-ec:aws:securityagent:integration`

È possibile utilizzare il contesto di crittografia per definire la politica delle chiavi KMS in base a tipi di risorse specifici. Per ulteriori informazioni, consulta the section called “Autorizzazioni KMS richieste”.

Default encryption (Crittografia di default)

Quando si crea una risorsa senza specificare una chiave gestita dal cliente, AWS Security Agent crittografa la risorsa utilizzando chiavi di crittografia AWS gestite fornite dai servizi di storage sottostanti (Amazon DynamoDB e Amazon S3). Non è richiesta alcuna configurazione aggiuntiva per la crittografia predefinita.

Chiave KMS predefinita per le applicazioni

È possibile impostare una chiave KMS predefinita a livello di applicazione. Quando viene configurata una chiave KMS predefinita, AWS Security Agent la utilizza come riserva per nuovi Agent Spaces e integrazioni quando non si specifica esplicitamente una chiave KMS durante la creazione delle risorse.

Per impostare una chiave KMS predefinita, specifica il `defaultKmsKeyId` parametro durante la creazione o l'aggiornamento dell'applicazione utilizzando la AWS CLI o l'SDK. La console richiede di specificare una chiave KMS predefinita durante la configurazione dell'applicazione.

Quando specifichi esplicitamente una chiave KMS durante la creazione delle risorse, questa ha la precedenza sull'impostazione predefinita a livello di applicazione.

Prerequisiti

Prima di configurare una chiave gestita dal cliente, completa i seguenti prerequisiti:

- Crea una chiave KMS di crittografia simmetrica in KMS. AWS La chiave deve soddisfare i seguenti requisiti:
  - Tipo di chiave: simmetrica
  - Utilizzo della chiave: crittografa e decrittografa
  - Specifiche chiave: `SYMMETRIC_DEFAULT`
  - Stato chiave: abilitato

  Per istruzioni, consulta Creating keys nella AWS Key Management Service Developer Guide.
- Configura la politica delle chiavi KMS e le politiche IAM per concedere a AWS Security Agent le autorizzazioni richieste. Per informazioni dettagliate, vedi the section called "Autorizzazioni KMS richieste".

Autorizzazioni KMS richieste

AWS Security Agent richiede le autorizzazioni KMS in due scenari:

- Crittografia dei dati all'interno AWS di Security Agent: quando si specifica una chiave gestita dal cliente per un Agent Space o un'integrazione, il servizio necessita delle autorizzazioni per utilizzare tale chiave per le operazioni di crittografia sui dati.
- Utilizzo CMK-encrypted AWS delle risorse: quando fornisci AWS risorse crittografate con una chiave gestita dal cliente (come bucket S3, gruppi di log CloudWatch Logs o segreti di Secrets Manager), il servizio necessita delle autorizzazioni per utilizzare tali chiavi per accedere alle risorse crittografate.

AWS Security Agent accede alla chiave KMS utilizzando identità diverse a seconda dell'operazione:

- AWS Operazioni della console di gestione: quando gli amministratori creano o gestiscono risorse nella console di AWS gestione (ad esempio, creando un Agent Space o aggiornando un'applicazione), il servizio utilizza il ruolo di amministratore per chiamare KMS. AWS
- Operazioni delle applicazioni Web: quando gli utenti di IAM Identity Center accedono ai dati tramite l'applicazione Web AWS Security Agent (ad esempio, visualizzando i risultati dei test di

penetrazione o avviando un test di penetrazione), il servizio utilizza il ruolo dell'applicazione creato durante la configurazione del AWS Security Agent per chiamare KMS. AWS

- Accesso alle risorse fornite dal cliente: quando il servizio accede alle AWS risorse fornite dal cliente durante i test di penetrazione (come i bucket S3, i gruppi di CloudWatch log Logs e i segreti di Secrets Manager), utilizza il ruolo del servizio di test di penetrazione per chiamare KMS. AWS
- Flussi di lavoro asincroni: per le operazioni in background eseguite al di fuori di qualsiasi sessione utente (ad esempio, esecuzione di test di penetrazione, elaborazione della revisione del codice e rotazione delle chiavi di filiale), il servizio utilizza il proprio service principal (`securityagent.amazonaws.com`) per chiamare AWS KMS per conto dell'utente.

Le sezioni seguenti descrivono le autorizzazioni richieste per ogni identità.

Policy della chiave

La politica della chiave KMS deve concedere a AWS Security Agent l'autorizzazione a utilizzare la chiave per operazioni crittografiche. Le dichiarazioni politiche chiave richieste dipendono dai tipi di risorse che intendi crittografare e dalle CMK-encrypted AWS risorse che fornisci al servizio.

Politica chiave per Agent Spaces

La seguente politica chiave concede a AWS Security Agent le autorizzazioni necessarie per crittografare e decrittografare i dati di Agent Space, inclusi i risultati dei test di penetrazione e le schermate.

Sostituisci i seguenti valori segnaposto nella policy:

- *111122223333* — L'ID del tuo account AWS
- *MyRole* — Il ruolo IAM che usi per gestire AWS Security Agent nella console
- *MyApplicationRole* — Il ruolo dell'applicazione creato durante la configurazione del AWS Security Agent
- *us-east-1* — La AWS regione in cui si utilizza AWS Security Agent

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKeyMetadataValidationForApplicationAndAgentSpaces",
      "Effect": "Allow",
```

```
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyRole"
      },
      "Action": [
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowUseOfHierarchicalKeyringForAgentSpaces",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyRole"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:agent-space":
"arn:aws:securityagent:us-east-1:111122223333:agent-space/*"
        },
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowSynchronousDataAccessForAgentSpaces",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyApplicationRole"
      },
      "Action": [
        "kms:GenerateDataKey",
```

```
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:agent-space":
"arn:aws:securityagent:us-east-1:111122223333:agent-space/*"
        },
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowAsynchronousDataAccessForAgentSpaces",
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:agent-space":
"arn:aws:securityagent:us-east-1:111122223333:agent-space/*"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:securityagent:us-east-1:111122223333:agent-space/*"
        }
      }
    },
    {
      "Sid": "AllowAsynchronousDataAccessForCodeRemediation",
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": [
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Important**
>
> Per ruotare le chiavi di filiale, è necessario che la politica delle chiavi KMS `kms:GenerateDataKeyWithoutPlaintext` conceda e `kms:ReEncryptFrom` le autorizzazioni al responsabile del servizio AWS Security Agent (`securityagent.amazonaws.com`), altrimenti la rotazione delle chiavi di filiale avrà esito negativo. `kms:ReEncryptTo` Per ulteriori informazioni sulle autorizzazioni richieste, consulta Ruotare una chiave di filiale.

Politica chiave per le integrazioni

La seguente politica chiave concede a AWS Security Agent le autorizzazioni necessarie per crittografare e decrittografare i dati di integrazione, inclusi i risultati della revisione del codice.

Sostituisci i seguenti valori segnaposto nella policy:

- *`111122223333`* — L'ID del tuo account AWS
- *`MyRole`* — Il ruolo IAM che usi per gestire AWS Security Agent nella console
- *`us-east-1`* — La AWS regione in cui usi AWS Security Agent

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKeyAccessValidationForIntegrations",
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::111122223333:role/MyRole"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
```

```
        "kms:Encrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws-crypto-ec:aws:securityagent:integration":
"arn:aws:securityagent:us-east-1:111122223333:integration/*"
        },
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowKeyMetadataValidationForIntegrations",
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "kms:DescribeKey",
      "Resource": "*"
    },
    {
      "Sid": "AllowAsynchronousDataAccessForIntegrations",
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:securityagent:us-east-1:111122223333:integration/*"
        },
        "StringLike": {
```

```
          "kms:EncryptionContext:aws-crypto-ec:aws:securityagent:integration":
 "arn:aws:securityagent:us-east-1:111122223333:integration/*"
        }
      }
    }
  ]
}
```

> **Note**
>
> È possibile combinare le dichiarazioni politiche chiave di Agent Space, integrazione e Security Requirement Pack in un'unica politica chiave se si desidera utilizzare la stessa chiave KMS per più tipi di risorse.

Politica chiave per i pacchetti di requisiti di sicurezza

La seguente politica chiave concede a AWS Security Agent le autorizzazioni necessarie per crittografare e decrittografare i dati del pacchetto dei requisiti di sicurezza. I pacchetti di requisiti di sicurezza non utilizzano un ruolo di applicazione Web. La policy utilizza due percorsi di accesso:

- Percorso sincrono: quando chiami l'API, il servizio utilizza le credenziali inoltrate per chiamare AWS KMS per tuo conto (tramite la condizione). `kms:ViaService`
- Percorso asincrono: per le operazioni asincrone in cui è possibile utilizzare i pacchetti, il servizio utilizza il proprio service principal per chiamare direttamente KMS. AWS

Sostituisci i seguenti valori nella politica:

- *`111122223333`* — L'ID AWS del tuo account
- *`MyRole`* — Il ruolo IAM che utilizzi per richiamare le operazioni del Security Requirement Pack
- *`us-east-1`* — La AWS regione in cui si utilizza AWS Security Agent

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKeyMetadataValidation",
      "Effect": "Allow",
```

```
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyRole"
      },
      "Action": [
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowUseOfHierarchicalKeyringForSecurityPacks",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyRole"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        },
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:security-requirement-pack":
"arn:aws:securityagent:us-east-1:111122223333:security-requirement-pack/*"
        }
      }
    },
    {
      "Sid": "AllowAsynchronousDataAccessForSecurityPacks",
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
```

```
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:security-requirement-pack":
 "arn:aws:securityagent:us-east-1:111122223333:security-requirement-pack/*"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:securityagent:us-east-1:111122223333:security-
requirement-pack/*"
        }
      }
    }
  ]
}
```

La politica contiene tre dichiarazioni:

- AllowKeyMetadataValidation— Garantisce `kms:DescribeKey` che AWS Security Agent possa convalidare che la chiave gestita dal cliente esiste, è abilitata e utilizza la crittografia simmetrica quando si specifica una CMK durante la creazione delle risorse. Utilizza la `kms:ViaService` condizione per garantire che la chiamata provenga dal servizio.
- AllowUseOfHierarchicalKeyringForSecurityPacks— Concede `kms:GenerateDataKeyWithoutPlaintext` (crea nuove chiavi di ramo), `kms:ReEncryptFrom` (ruota le chiavi di ramo esistenti) `kms:ReEncryptTo` e `kms:Decrypt` (recupera le chiavi di ramo esistenti) per le operazioni gerarchiche con portachiavi. Queste operazioni utilizzano le credenziali inoltrate attraverso il percorso sincrono e rientrano nell'ambito delle risorse del Security Requirement Pack in base alla condizione del contesto di crittografia.
- AllowAsynchronousDataAccessForSecurityPacks— Concedekms:GenerateDataKeyWithoutPlaintext, `kms:Decryptkms:ReEncryptTo`, e `kms:ReEncryptFrom` al responsabile del servizio AWS Security Agent per operazioni asincrone quando non sono disponibili le credenziali del chiamante.

A differenza della policy chiave di Agent Spaces, la policy del Security Requirement Pack non include un responsabile del ruolo dell'applicazione Web. È possibile accedere ai pacchetti dei requisiti di sicurezza tramite la Console di AWS gestione utilizzando il ruolo di amministratore, non tramite

l'applicazione Web AWS Security Agent. Tutte le operazioni sincrone utilizzano il ruolo di chiamante singolo (via`kms:ViaService`).

> **Note**
>
> Se si utilizza la stessa chiave KMS sia per Agent Spaces che per i pacchetti di requisiti di sicurezza, è possibile combinare le dichiarazioni politiche chiave di entrambe le sezioni in un'unica politica chiave.

Politica chiave per CMK-encrypted AWS risorse

Se si forniscono AWS risorse crittografate con una chiave gestita dal cliente a AWS Security Agent, è necessario aggiornare la politica delle chiavi sulla chiave KMS di ciascuna risorsa per concedere le autorizzazioni necessarie. Questo vale per le seguenti risorse:

- Bucket S3: se fornisci risorse didattiche da un bucket S3 crittografato con una chiave gestita dal cliente (SSE-KMS), la policy chiave deve consentire al ruolo del servizio di test di penetrazione di decrittografare gli oggetti.
- Segreti di Secrets Manager: se le credenziali del test di penetrazione sono archiviate nei segreti di Secrets Manager crittografati con una chiave gestita dal cliente, la policy chiave deve consentire al ruolo del servizio di test di penetrazione di decrittografare tali segreti. Se l'applicazione Web crea segreti per conto dell'utente, la policy chiave deve consentire anche al ruolo dell'applicazione di crittografare tali segreti.
- CloudWatch Gruppi di log di log: se il gruppo di log CloudWatch Logs utilizzato per archiviare i log di esecuzione dei test di penetrazione è crittografato con una chiave gestita dal cliente, la policy di chiave deve consentire a CloudWatch Logs di convalidare la chiave KMS tramite il ruolo di servizio e consentire al responsabile del servizio Logs di eseguire operazioni crittografiche. CloudWatch

> **Important**
>
> AWS Security Agent può anche creare gruppi di log CloudWatch Logs e Secrets Manager segreti per conto dell'utente. Quando configuri la politica delle chiavi KMS, includi anche le istruzioni corrispondenti per queste risorse create dal servizio.

Le seguenti dichiarazioni politiche chiave concedono le autorizzazioni necessarie per le risorse. CMK-encrypted Includi solo le istruzioni che si applicano alla tua configurazione. Se una risorsa utilizza la stessa chiave KMS specificata per Agent Space, aggiungi queste istruzioni alla politica di quella chiave. Se una risorsa utilizza una chiave KMS diversa, aggiungi invece queste istruzioni alla politica di quella chiave.

Sostituisci i seguenti valori segnaposto nella politica:

- *111122223333* — L'ID del tuo account AWS
- *MyApplicationRole* — Il ruolo dell'applicazione creato durante la configurazione AWS di Security Agent
- *MyPenTestServiceRole* — Il ruolo del servizio di penetration test
- *us-east-1* — La AWS regione in cui si utilizza AWS Security Agent

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKmsKeyAccessForCreatingSecrets",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyApplicationRole"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:*"
        }
      }
    },
    {
```

```
      "Sid": "AllowKmsKeyDecryptionForS3Objects",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyPenTestServiceRole"
      },
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "s3.*.amazonaws.com",
          "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::YOUR-BUCKET-NAME*"
        }
      }
    },
    {
      "Sid": "AllowKmsKeyDecryptionForSecretsManagerSecrets",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyPenTestServiceRole"
      },
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:YOUR-SECRET-NAME*"
        }
      }
    },
    {
      "Sid": "AllowKmsKeyValidationForCloudWatchLogsLogGroups",
      "Effect": "Allow",
      "Principal": {
```

```
        "AWS": "arn:aws:iam::111122223333:role/MyPenTestServiceRole"
      },
      "Action": [
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "logs.*.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowKmsKeyAccessForCloudWatchLogsLogGroups",
      "Effect": "Allow",
      "Principal": {
        "Service": "logs.us-east-1.amazonaws.com"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:EncryptionContext:aws:logs:arn": "arn:aws:logs:us-
east-1:111122223333:log-group:YOUR-LOG-GROUP-NAME*"
        }
      }
    }
  ]
}
```

Note

- L'`AllowKmsKeyDecryptionForS3Objects`istruzione è richiesta solo se fornisci risorse didattiche provenienti da bucket S3 crittografati con una chiave gestita dal cliente. Per ulteriori informazioni sulla configurazione SSE-KMS per S3, consulta Proteggere i dati con. SSE-KMS
- L'`AllowKmsKeyDecryptionForSecretsManagerSecrets`istruzione è richiesta solo se le credenziali del penetration test sono archiviate nei segreti di Secrets Manager crittografati con una chiave gestita dal cliente. Il ruolo di servizio richiede l'accesso per decrittografare i segreti durante i test di penetrazione. Per ulteriori informazioni sulla crittografia segreta, vedere Crittografia e decrittografia segrete in Secrets Manager.
- L'`AllowKmsKeyValidationForCloudWatchLogsLogGroups`istruzione concede il ruolo di servizio `kms:DescribeKey` in modo che CloudWatch Logs possa convalidare la chiave KMS tramite il ruolo di servizio quando la associa a un gruppo di log.
- L'`AllowKmsKeyAccessForCreatingSecrets`istruzione è richiesta se l'applicazione Web crea segreti di Secrets Manager per conto dell'utente utilizzando una chiave gestita dal cliente. Il ruolo dell'applicazione deve `kms:GenerateDataKey` `kms:Decrypt` crittografare il segreto con la tua chiave KMS.
- L'`AllowKmsKeyAccessForCloudWatchLogsLogGroups`istruzione concede al servizio CloudWatch Logs principal (`logs.`*`us-east-1`*`.amazonaws.com`) le autorizzazioni necessarie per crittografare e decrittografare i dati di registro. Questa dichiarazione è richiesta anche se AWS Security Agent crea un gruppo di log per conto dell'utente quando non ne fornisce uno esistente. Per ulteriori informazioni, consulta Crittografare i dati di registro nei CloudWatch registri utilizzando AWS KMS.
- Se più risorse condividono la stessa chiave KMS, puoi combinare le istruzioni in un'unica politica chiave.

Ruolo di amministratore

Non è richiesta alcuna policy IAM aggiuntiva per il ruolo di amministratore (il ruolo IAM utilizzato per gestire AWS Security Agent nella console).

Ruolo dell'applicazione

Oltre alla policy chiave KMS, collega la seguente politica IAM al ruolo dell'applicazione specificato durante la configurazione del AWS Security Agent. Questa politica concede le autorizzazioni di ruolo per utilizzare le chiavi gestite dai clienti per crittografare e decrittografare i dati di Agent Space e creare segreti in Secrets Manager. AWS

Sostituisci i seguenti valori segnaposto nella policy:

- *111122223333* — L'ID del tuo account AWS
- *us-east-1* — La AWS regione in cui usi AWS Security Agent
- Gli ARN della chiave KMS`Resource`: gli ARN delle tue chiavi KMS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSynchronousDataAccessForAgentSpaces",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890cd"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333",
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        },
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:agent-space":
 "arn:aws:securityagent:us-east-1:111122223333:agent-space/*"
        }
      }
    },
    {
      "Sid": "AllowKmsKeyAccessForCreatingSecrets",
      "Effect": "Allow",
```

```
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890cd"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:*"
        }
      }
    }
  ]
}
```

> **Note**
>
> Il ruolo dell'applicazione è un ruolo IAM specificato dall'utente o creato dalla console durante AWS la configurazione del Security Agent. L'applicazione web assume questo ruolo per recuperare i log di esecuzione dei test di penetrazione e creare segreti di Secrets Manager per conto dell'utente.
>
> - L'`AllowKmsKeyAccessForCreatingSecrets`istruzione è necessaria se si configurano le risorse di autenticazione per i test di penetrazione e si sceglie di inserire direttamente le credenziali anziché specificare un segreto esistente. L'applicazione Web crea un segreto per conto dell'utente e il ruolo dell'applicazione necessita delle autorizzazioni contenute in questa istruzione per crittografare il segreto con la chiave gestita dal cliente specificata per Agent Space. Aggiorna gli `Resource` ARN in questa istruzione in modo che corrispondano alla chiave KMS utilizzata per Agent Space.

Ruolo del servizio

Durante i test di penetrazione, AWS Security Agent si assume il ruolo di servizio di penetration test per accedere alle risorse dell'utente. AWS Se una di queste risorse è crittografata con una chiave gestita dal cliente, è necessario concedere al ruolo di servizio le autorizzazioni per utilizzare le chiavi KMS corrispondenti. Questo vale per le seguenti risorse:

- Bucket S3: se fornisci risorse di apprendimento (come documenti API, modelli di minaccia o codice sorgente) da un bucket S3 crittografato con una chiave gestita dal cliente, il ruolo di servizio necessita delle autorizzazioni per decrittografare gli oggetti in quel bucket. Per ulteriori informazioni sulla configurazione SSE-KMS per S3, consulta Protezione dei dati con. SSE-KMS
- Segreti di Secrets Manager: se le credenziali del penetration test sono archiviate nei segreti di Secrets Manager crittografati con una chiave gestita dal cliente, il ruolo di servizio necessita delle autorizzazioni per decrittografare tali segreti. Per ulteriori informazioni sulla crittografia segreta, vedere Crittografia e decrittografia segrete in Secrets Manager.
- CloudWatch Gruppi di log: se il gruppo di log CloudWatch Logs utilizzato per archiviare i log di esecuzione dei penetration test è crittografato con una chiave gestita dal cliente (inclusi i gruppi di log creati da AWS Security Agent per conto dell'utente), il ruolo di servizio `kms:DescribeKey` necessita dell'autorizzazione per convalidare la chiave. Il responsabile del servizio CloudWatch Logs gestisce la crittografia e la decrittografia effettive dei dati di registro e tali autorizzazioni vengono concesse tramite la politica chiave (vedi). the section called “Policy della chiave” Per ulteriori informazioni sulla crittografia dei dati di registro, consulta Crittografare i dati di registro nei registri utilizzando KMS. CloudWatch AWS

> **Important**
>
> Se utilizzi una chiave KMS diversa per crittografare queste risorse rispetto a quella specificata per Agent Space, devi concedere le autorizzazioni del ruolo di servizio per ogni chiave KMS che protegge una risorsa a cui il ruolo di servizio accede durante i test di penetrazione.

Allega la seguente policy IAM al ruolo del servizio di penetration test. Includi solo le istruzioni che si applicano alla tua configurazione.

Sostituisci i seguenti valori segnaposto nella politica:

- *111122223333* — L'ID del tuo account AWS

- *us-east-1* — La AWS regione in cui usi AWS Security Agent
- Gli ARN della chiave KMS in ingressoResource: gli ARN delle chiavi gestite dal cliente utilizzati per crittografare ogni risorsa

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKmsAccessForEncryptedS3Buckets",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE-S3-KEY-ID"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "s3.*.amazonaws.com",
          "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::YOUR-BUCKET-NAME*"
        }
      }
    },
    {
      "Sid": "AllowKmsAccessForEncryptedSecrets",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE-SECRETS-KEY-ID"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "secretsmanager.*.amazonaws.com",
```

```
          "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:YOUR-SECRET-NAME*"
        }
      }
    },
    {
      "Sid": "AllowKmsKeyValidationForCloudWatchLogsLogGroups",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE-CLOUDWATCH-LOGS-KEY-ID"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "logs.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Note

- L'`AllowKmsAccessForEncryptedS3Bucket`istruzione è richiesta solo se fornisci risorse di apprendimento provenienti da bucket S3 crittografati con una chiave gestita dal cliente. Aggiorna l'`Resource`ARN in modo che corrisponda alla chiave KMS utilizzata per crittografare il bucket S3 e aggiorna il `kms:EncryptionContext:aws:s3:arn` valore in modo che corrisponda al nome del bucket.
- L'`AllowKmsAccessForEncryptedSecrets`istruzione è richiesta solo se le credenziali del penetration test sono archiviate nei segreti di Secrets Manager crittografati con una chiave gestita dal cliente. Aggiorna l'`Resource`ARN in modo che corrisponda alla chiave KMS utilizzata per crittografare i tuoi segreti e aggiorna il `kms:EncryptionContext:SecretARN` valore in modo che corrisponda al tuo nome segreto.

- L'`AllowKmsKeyValidationForCloudWatchLogsLogGroups`istruzione è richiesta solo se il gruppo di log CloudWatch Logs è crittografato con una chiave gestita dal cliente, inclusi i gruppi di log creati da AWS Security Agent per tuo conto. Aggiorna l'`Resource`ARN in modo che corrisponda alla chiave KMS utilizzata per crittografare il gruppo di log.
- Se più risorse condividono la stessa chiave KMS, puoi combinare le istruzioni ed elencare l'ARN della chiave condivisa `Resource` una volta sul campo.

Crea una risorsa con una chiave gestita dal cliente

È possibile specificare una chiave gestita dal cliente durante la configurazione di AWS Security Agent o durante la creazione di singole risorse. La chiave KMS crittografa tutti i dati appartenenti a quella risorsa e alle sue sottorisorse.

Imposta una chiave KMS predefinita durante la configurazione (console)

È possibile configurare una chiave KMS predefinita durante la configurazione iniziale di AWS Security Agent. Questa chiave viene utilizzata come predefinita per i nuovi Agent Spaces e le integrazioni, a meno che non si specifichi una chiave diversa.

1. Nella pagina Configurazione di AWS Security Agent, espandi la sezione Crittografia - opzionale.
2. Seleziona Personalizza le impostazioni di crittografia (avanzate).
3. Per Scegli una chiave AWS KMS, seleziona una chiave KMS dal tuo account o inserisci una chiave KMS ARN.
4. Completa i passaggi di configurazione rimanenti e scegli Configura AWS Security Agent.

AWS Security Agent convalida la chiave KMS per confermare che esiste, è abilitata e utilizza la crittografia simmetrica. Se la convalida fallisce, l'installazione non procede e viene visualizzato un messaggio di errore.

Crea un Agent Space con una chiave gestita dal cliente (console)

1. Nella console AWS Security Agent, vai alla pagina Agent Spaces.
2. Scegli Create Agent Space.
3. Inserisci un nome e una descrizione opzionale per il tuo Agent Space.

4. Espandere la sezione Advanced (Avanzate).
5. In Crittografia dei dati, scegli una delle seguenti opzioni:
   - Usa la chiave predefinita dell'applicazione: utilizza la chiave KMS predefinita configurata durante la configurazione AWS di Security Agent. Questa opzione è selezionata per impostazione predefinita se è configurata una chiave predefinita.
   - Usa una chiave diversa: specifica una chiave KMS diversa per questo Agent Space. Seleziona Personalizza le impostazioni di crittografia (avanzate), quindi per Scegli una chiave AWS KMS, seleziona una chiave KMS dal tuo account o inserisci un ARN.
6. Scegli Create (Crea).

Crea un'integrazione con una chiave gestita dal cliente (console)

1. Nella console AWS Security Agent, vai alla pagina Integrazioni.
2. Scegli Aggiungi integrazione e seleziona il tuo provider (ad esempio, GitHub).
3. Completa il passaggio 1: installa e autorizza l'applicazione del provider.
4. Nel passaggio 2: Registra i dettagli, inserisci un nome di registrazione e configura le impostazioni del provider.
5. Nella sezione Crittografia dei dati, seleziona Personalizza le impostazioni di crittografia (avanzate).
6. Per Scegli una chiave AWS KMS, seleziona una chiave KMS dal tuo account o inserisci una chiave KMS ARN.
7. Scegli Connetti.

Crea una risorsa con una chiave gestita dal cliente (AWS CLI o SDK)

Per specificare una chiave gestita dal cliente utilizzando la AWS CLI o l'SDK:

- Includi il `defaultKmsKeyId` parametro durante la chiamata `CreateApplication` per impostare una chiave KMS predefinita per la tua applicazione. Questa chiave viene utilizzata come riserva durante la creazione di Agent Spaces o integrazioni senza una chiave KMS esplicita.
- Includi il `kmsKeyId` parametro durante la chiamata `CreateAgentSpace` o `CreateIntegration` per crittografare una risorsa specifica. Questo ha la precedenza sull'impostazione predefinita a livello di applicazione.

Per i dettagli sui parametri, consulta la Guida di riferimento alle API di AWS Security Agent.

Se non si specifica una chiave KMS, AWS Security Agent utilizza la chiave KMS predefinita a livello di applicazione, se configurata. In caso contrario, la risorsa viene crittografata con chiavi gestite. AWS

Rotazione delle chiavi

AWS Security Agent ruota automaticamente le chiavi delle filiali su base periodica. La rotazione della chiave di ramo crea una nuova versione attiva della chiave di ramo mantenendo tutte le versioni precedenti. Dopo la rotazione:

- I nuovi dati vengono crittografati con la nuova versione della chiave di filiale.
- I dati precedentemente crittografati rimangono decifrabili utilizzando la versione precedente della chiave di filiale.
- Non è richiesta una nuova crittografia dei dati.

La rotazione delle chiavi Branch è separata dalla rotazione delle chiavi KMS. Puoi abilitare la rotazione automatica delle chiavi KMS per la chiave gestita dal cliente in modo indipendente. Per ulteriori informazioni, consulta Rotating KMS keys nella AWS Key Management Service Developer Guide.

Dopo una rotazione della chiave di filiale, c'è un breve periodo durante il quale le copie memorizzate nella cache della chiave di filiale precedente possono ancora essere utilizzate per nuove operazioni di crittografia. Questa finestra è determinata dal time-to-live (TTL) della cache interna e non influisce sulla sicurezza dei dati.

Considerazioni

Tieni presente quanto segue quando utilizzi le chiavi gestite dal cliente con AWS Security Agent:

- Le chiavi gestite dal cliente si applicano solo alle nuove risorse. Le risorse esistenti create prima di configurare una chiave gestita dal cliente continuano a utilizzare la AWS crittografia gestita. Non è prevista alcuna migrazione dei dati esistenti.
- Le chiavi gestite dal cliente vengono specificate al momento della creazione. La chiave KMS viene specificata durante la creazione di una risorsa. Non è possibile aggiungere o modificare la chiave KMS per una risorsa esistente.
- Sono supportate più chiavi KMS. Puoi utilizzare chiavi KMS diverse per risorse diverse. Ad esempio, è possibile utilizzare una chiave per gli Agent Spaces di produzione e una chiave diversa per gli Agent Spaces di sviluppo.

- La disabilitazione o l'eliminazione di una chiave KMS rende i dati inaccessibili. Se si disabilita o si pianifica l'eliminazione di una chiave KMS, AWS Security Agent non può decrittografare i dati crittografati con tale chiave. Le risorse interessate diventano inaccessibili finché la chiave non viene riattivata. L'eliminazione di una chiave KMS impedisce in modo permanente l'accesso a tutti i dati crittografati con tale chiave.
- Sono richieste le autorizzazioni chiave relative alle policy. Se rimuovi le autorizzazioni richieste dalla politica delle chiavi KMS, AWS Security Agent non può accedere ai dati crittografati. Assicurati che la politica chiave conceda le autorizzazioni per il ruolo di amministratore (utilizzato per gestire il servizio nella AWS Console), il ruolo dell'applicazione (utilizzato dall'applicazione Web), il ruolo del servizio di test di penetrazione (assunto dagli agenti per eseguire i test di penetrazione) e il responsabile del servizio AWS Security Agent, come descritto in. the section called “Autorizzazioni KMS richieste”
- AWS Si applicano le quote KMS. Le operazioni crittografiche sulla chiave KMS contano ai fini delle quote di richiesta AWS KMS. In condizioni di utilizzo normale, l'architettura gerarchica del portachiavi riduce al minimo le chiamate KMS tramite la memorizzazione nella cache delle chiavi di filiale. Per ulteriori informazioni, consulta Request quotas nella Key Management Service Developer Guide. AWS

Risoluzione dei problemi

Trova soluzioni agli errori più comuni quando usi AWS Security Agent.

Accesso negato: il tipo di GitHub account selezionato non è corretto o il nome dell'organizzazione specificato non è corretto

- Hai installato l'applicazione AWS Security Agent nell' GitHub organizzazione desiderata ma l'hai erroneamente impostata su `User` invece `GitHub Account Type` di `Organization`
- Hai installato l'applicazione AWS Security Agent nell' GitHub organizzazione desiderata e l'`GitHub Account Type`hai impostata correttamente, `Organization` ma hai lasciato il `Organization Name` campo vuoto o inserito un nome dell'organizzazione errato che non corrisponde all'organizzazione in cui hai installato l'applicazione.

Soluzione::

1. Accedi GitHub e disinstalla l'app dall'organizzazione. Per ulteriori informazioni, consulta the section called “Fase 1: Disinstalla l' GitHub app AWS Security Agent da GitHub”.

2. Torna alla pagina delle integrazioni e riavvia il processo di integrazione facendo clic su`Add Integrations`, installa e autorizza nuovamente l'app nell' GitHub organizzazione desiderata.
3. Seleziona `Organization` dal menu a discesa di `GitHub account type`
4. Assicurati che l'`Organization Name`input sia ESATTAMENTE uguale a quello in cui hai installato l'applicazione.
5. Scegli Connect per creare GitHub l'integrazione della tua organizzazione.

Accesso negato: autorizzazioni insufficienti per installare GitHub l'app nell'organizzazione

Quando tenti di installare l'applicazione AWS Security Agent nell' GitHub organizzazione desiderata, vedrai due diversi messaggi sul pulsante nella pagina di installazione.

- Un'organizzazione `Member` vedrà `Authorize & Request`
- Un'organizzazione `Owner` vedrà `Install & Authorize`

Puoi verificare se appartieni `Member` o fai parte `Owner` dell' GitHub organizzazione seguendo i passaggi seguenti.

1. Vai su github.com
2. Scegli il tuo profilo sul sito web
3. Vai `Organizations` al menu a discesa e selezionalo
4. Trova l'organizzazione in cui desideri installare AWS Security Agent dall'elenco delle organizzazioni, specificherà se appartieni al nome dell'organizzazione `Member` o lo trovi `Owner` accanto.

Possibili soluzioni:

- Chiedi a un proprietario di approvare la tua richiesta di installazione PRIMA di provare a creare l'integrazione
- Chiedi a un proprietario di aggiornare il tuo ruolo nell' GitHub organizzazione da un punto `Member` a uno `Owner` e di riavviare nuovamente il processo di integrazione

L'agente non può connettersi all'endpoint durante un test di penetrazione

Se l'agente del penetration test non è in grado di effettuare chiamate all'URL di destinazione configurato o non riesce a navigare correttamente nell'endpoint di destinazione:

- Se l'endpoint effettua chiamate a domini esterni all'URL di destinazione configurato, verifica che i domini aggiuntivi vengano aggiunti come URL accessibili nella configurazione pentest
- I test di penetrazione sono attualmente disponibili solo per gli HTTP/HTTPS endpoint che servono traffico sulle porte 80 o 443
- Se hai configurato un WAF, verifica che il WAF non stia bloccando il traffico dei penetration test. Puoi consentire l'elenco del traffico dei test di penetrazione per `User-Agent` intestazione, che per impostazione predefinita sarà impostato su `securityagent`

Ottenere ulteriore assistenza

Se continui a riscontrare problemi dopo aver provato questi passaggi per la risoluzione dei problemi:

- Controlla la pagina di stato del servizio AWS Security Agent
- Contatta AWS Support per ricevere assistenza su problemi di configurazione complessi

Per utenti e sviluppatori (app web e IDE)

Esegui revisioni progettuali, modelli di minaccia, revisioni del codice e test di penetrazione nell'applicazione web, in un IDE o in un provider di sorgenti connesse, quindi esamina e correggi i risultati.

Accedi all'app Web AWS Security Agent

È necessario accedere all'app Web AWS Security Agent per completare attività come:

- Esegui una revisione del progetto
- Eseguire un test di penetrazione

Metodi di accesso

AWS Security Agent offre diversi metodi per accedere all'applicazione Web, a seconda di come l'organizzazione ha configurato l'accesso durante la configurazione iniziale e se disponi dell'accesso alla console AWS.

IAM Identity Center (SSO): se la tua organizzazione ha abilitato IAM Identity Center, puoi accedere utilizzando le tue credenziali SSO. Devi essere assegnato ad almeno un Agent Space in IAM Identity Center prima di poter accedere all'applicazione web.

Accesso amministratore (IAM): se disponi dell'accesso alla console AWS con le autorizzazioni appropriate, puoi avviare l'applicazione Web tramite il link di accesso amministratore su qualsiasi pagina di Agent Space. Questo metodo fornisce l'autenticazione tramite la sessione esistente della console.

> **Note**
>
> Il metodo di accesso principale utilizzato dall'organizzazione è stato determinato durante la configurazione iniziale di AWS Security Agent. Per informazioni sulla configurazione dell'accesso e delle assegnazioni degli utenti, consulta. the section called “Concedi agli utenti l'accesso all'app Web AWS Security Agent”

Accedi con IAM Identity Center (SSO)

Se la tua organizzazione ha configurato l'accesso a IAM Identity Center, puoi accedere all'applicazione web utilizzando le tue credenziali SSO attraverso più punti di ingresso.

Prerequisiti

- Ti è stato assegnato almeno un Agent Space in IAM Identity Center
- Hai le tue credenziali SSO di IAM Identity Center

Accedi all'applicazione web

Scegli uno dei seguenti metodi in base alle tue esigenze:

Per visualizzare tutti gli Agent Spaces a cui sei assegnato:

1. Nella console AWS Security Agent, accedi a Impostazioni.
2. Individua il dominio dell'applicazione Web e copia l'URL.

> **Tip**
>
> Aggiungi questo URL ai preferiti per un facile accesso. Questo è il punto di accesso universale per visualizzare tutti gli Agent Spaces a cui sei assegnato.

3. Vai all'URL dell'applicazione web.
4. Inserisci le tue credenziali IAM Identity Center quando richiesto.
5. Dopo l'autenticazione, vedrai un elenco di tutti gli Agent Spaces a cui sei assegnato.
6. Seleziona l'Agent Space in cui vuoi lavorare.

Per accedere direttamente a uno specifico Agent Space (richiede l'accesso alla console AWS):

1. Accedi alla Console di gestione AWS.
2. Accedi alla console AWS Security Agent.
3. Accedi all'Agent Space a cui desideri accedere.
4. Seleziona una delle seguenti opzioni:
   - Avvia il pulsante dell'applicazione Web nella pagina di panoramica di Agent Space

- Avvia il pulsante dell'app Web nella sezione di revisione del codice
- Avvia il pulsante dell'app web nella sezione Penetration testing

5. Inserisci le tue credenziali IAM Identity Center quando richiesto.
6. Dopo l'autenticazione, verrai indirizzato direttamente a quell'Agent Space nell'applicazione web.

> **Note**
>
> Se non disponi dell'accesso alla console AWS, utilizza il dominio dell'applicazione Web dalla pagina Impostazioni per accedere a tutti gli Agent Space assegnati.

Accedi con accesso da amministratore (IAM)

Se disponi dell'accesso alla console AWS con le autorizzazioni AWS Security Agent appropriate, puoi avviare l'applicazione Web tramite il link di accesso amministratore con autenticazione automatica.

Prerequisiti

- Hai effettuato l'accesso alla Console di gestione AWS
- Disponi delle autorizzazioni appropriate per accedere alle risorse di AWS Security Agent

Accedi all'applicazione web

Seleziona uno dei seguenti metodi:

Per accedere a uno specifico Agent Space:

1. Accedi alla Console di gestione AWS.
2. Accedi alla console AWS Security Agent.
3. Accedi all'Agent Space a cui desideri accedere.
4. Scegli il pulsante di accesso come amministratore nella pagina di panoramica di Agent Space.
5. L'applicazione Web si apre in una nuova scheda con autenticazione automatica per quell'Agent Space.

> **Note**
>
> Il pulsante di accesso amministratore è sempre disponibile per gli utenti con accesso alla console AWS, indipendentemente dal fatto che l'organizzazione utilizzi IAM Identity Center come metodo di accesso principale.

Crea una revisione del design

Valuta i tuoi documenti di progettazione rispetto ai requisiti di sicurezza dell'organizzazione caricando file da sottoporre a revisione da parte di AWS Security Agent. Le revisioni dei progetti aiutano a identificare i problemi di sicurezza nelle prime fasi del ciclo di vita dello sviluppo, consentendoti di affrontare i problemi di architettura nel momento in cui sono più convenienti da risolvere.

AWS Security Agent analizza i documenti di progettazione rispetto ai requisiti di sicurezza dell'organizzazione, fornendo risultati di sicurezza dettagliati per migliorare il livello di sicurezza prima che inizi l'implementazione.

In questa procedura, creerai una revisione del progetto caricando file di progettazione per l'analisi.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Accesso all'applicazione Web AWS Security Agent
- Documenti di progettazione pronti per il caricamento (DOC, DOCX, JPEG, MD, PDF, PNG e TXT)
- Ogni file deve pesare almeno 2 MB, con un totale combinato di 6 MB per tutti i file
- Comprensione dei requisiti di sicurezza consentiti per l'organizzazione

Fase 1: Iniziate a creare una revisione del progetto

Vai alla pagina di creazione della revisione del progetto nell'Agent Web App.

1. Accedi all'applicazione Web AWS Security Agent.
2. Vai alla sezione Recensioni dei design.
3. Scegli Create Design Review.

> **Tip**
>
> Puoi visualizzare i requisiti di sicurezza abilitati della tua organizzazione accedendo alla pagina Requisiti di sicurezza nella console AWS Security Agent. Seleziona qualsiasi requisito abilitato per visualizzarne i dettagli. Questi requisiti vengono utilizzati per analizzare i file di progettazione.

Fase 2: Assegna un nome alla recensione del progetto

Fornisci un nome descrittivo che aiuti a identificare lo scopo e l'ambito di questa revisione del progetto.

1. Nella sezione Nome della revisione del progetto, individuate il campo Nome.
2. Inserisci un nome descrittivo per la revisione del progetto.

> **Note**
>
> Il nome deve identificare chiaramente il progetto, la funzionalità o il componente oggetto della revisione. Massimo 80 caratteri.

Fase 3: Caricare i file di progettazione

Carica i documenti di progettazione che desideri che AWS Security Agent analizzi per la conformità alla sicurezza.

1. Nella sezione File da esaminare, esamina i requisiti del file:

> **Important**
>
> È possibile caricare un massimo di 5 file per revisione del progetto. Ogni file deve pesare almeno 2 MB, con un totale complessivo di 6 MB per tutti i file. Formati supportati: DOC, DOCX, JPEG, MD, PDF, PNG e TXT.

2. Carica i tuoi file utilizzando uno di questi metodi:
   a. Trascina e rilascia: trascina i file direttamente nell'area dropzone del file
   b. Sfoglia: utilizza il pulsante Scegli i file per sfogliare e selezionare i file dal tuo computer

3. Verifica che tutti i file richiesti siano caricati.

> **Tip**
>
> Per ottenere risultati ottimali, includete diagrammi di architettura, specifiche di progettazione e documentazione tecnica che descrivano i componenti e i flussi di dati rilevanti per la sicurezza del sistema.

Fase 4: Iniziare la revisione del progetto

Dopo aver configurato tutte le informazioni richieste, avviate l'analisi della sicurezza dei documenti di progettazione.

1. Controllate tutti i file e le impostazioni caricati per assicurarne la precisione.
2. Scegli Inizia la revisione del design.
3. AWS Security Agent analizza i documenti di progettazione rispetto ai requisiti di sicurezza abilitati.

> **Note**
>
> Il processo di revisione del progetto in genere viene completato in pochi minuti, a seconda del numero e della dimensione dei file caricati. Riceverai risultati sulla sicurezza in base ai requisiti di sicurezza della tua organizzazione.

Fasi successive

Dopo aver iniziato la revisione del progetto:

- Monitora lo stato di avanzamento della revisione nell'Agent Web App
- Esamina i risultati di sicurezza
- Condividi i risultati con il tuo team di sviluppo
- Risolvi i problemi di sicurezza identificati nel tuo progetto
- Aggiorna i documenti di progettazione e inviali nuovamente se necessario

Esamina i risultati di una revisione del progetto

I risultati della revisione aiutano a capire quali requisiti di sicurezza sono soddisfatti, quali richiedono attenzione e quali azioni intraprendere per migliorare il livello di sicurezza del progetto prima che inizi l'implementazione.

In questa procedura, imparerai come accedere, filtrare e interpretare i risultati della revisione del progetto per affrontare efficacemente i problemi di sicurezza.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Una revisione completa del progetto
- Accesso all'applicazione Web AWS Security Agent
- Familiarità con i requisiti di sicurezza abilitati della tua organizzazione

Fase 1: Accedere alla revisione del progetto

Passa alla revisione del progetto per visualizzare i risultati e le informazioni di riepilogo.

1. Accedi all'applicazione Web AWS Security Agent.
2. Vai alla sezione Recensioni dei design.
3. Seleziona la revisione del progetto che desideri esaminare dall'elenco.

> **Tip**
>
> La pagina dei dettagli della revisione del progetto mostra un riepilogo dello stato della revisione, della data di completamento e del numero di file esaminati.

Fase 2: Rivedi il riepilogo dei risultati

Esamina il riepilogo di alto livello per comprendere lo stato di sicurezza generale del tuo progetto.

1. Individua la sezione Riepilogo.
2. Controlla il conteggio per ogni categoria dello stato di conformità: Conforme Non-compliant, Dati insufficienti e Non applicabile.

> **Note**
>
> Il riepilogo fornisce i conteggi per ogni tipo di stato, aiutandoti a valutare rapidamente il numero di risultati che richiedono attenzione. Per spiegazioni dettagliate di ogni stato, consulta la Fase 4.

Fase 3: Filtrare e navigare tra i risultati

Utilizza le funzionalità di filtraggio e ricerca per concentrarti su risultati o stati di conformità specifici.

1. Nella sezione Rivedi i risultati, individua i controlli del filtro.
2. Per filtrare in base allo stato:
   a. Scegli il menu a discesa dello stato.
   b. Seleziona uno stato di conformità specifico per visualizzare solo i risultati con quello stato.
3. Per cercare requisiti di sicurezza specifici:
   a. Inserisci le parole chiave nel campo di ricerca.
   b. I risultati si aggiornano automaticamente durante la digitazione.
4. Usa i controlli di impaginazione per navigare tra più pagine di risultati.

> **Tip**
>
> Filtra innanzitutto per Non-compliantstato per dare priorità ai risultati che richiedono un'attenzione immediata nella progettazione.

Fase 4: Comprendi gli stati di conformità

Ogni risultato mostra uno stato di conformità che indica in che modo il progetto risponde a uno specifico requisito di sicurezza:

- Conforme: il design soddisfa i requisiti di sicurezza in base all'analisi
- Non-compliant— Il tuo design viola o soddisfa in modo inadeguato i requisiti di sicurezza
- Dati insufficienti: i file caricati non dispongono di informazioni sufficienti per determinare la conformità
- Non applicabile: il requisito di sicurezza non si applica alla progettazione del sistema

> **Important**
>
> Concentrati sugli stati dei dati Non-compliante su quelli insufficienti, poiché richiedono un'azione. Risolvi i problemi di non conformità aggiornando il progetto e risolvete i problemi relativi ai dati insufficienti caricando documentazione di progettazione aggiuntiva.

Fase 5: Visualizza i dettagli del ritrovamento

Seleziona i singoli risultati per visualizzare le linee guida dettagliate sulla giustificazione e sulla correzione.

1. Nella tabella dei risultati, seleziona il nome di un requisito di sicurezza.
2. Esamina i dettagli del risultato, che includono:
   - Il requisito di sicurezza specifico oggetto di valutazione
   - Un commento che spieghi il motivo per cui il risultato è stato raggiunto lo stato di conformità, compresi dettagli specifici sugli elementi mancanti o non conformi
   - Linee guida correttive consigliate per risolvere il problema
   - Collegamenti alla documentazione o agli standard interni dell'organizzazione per i requisiti di sicurezza

> **Note**
>
> Il commento spiega il ragionamento di AWS Security Agent con dettagli specifici. In caso di dati insufficienti, il commento identifica le informazioni mancanti, ad esempio «I documenti di progettazione non menzionano i meccanismi di autenticazione» o «Nessuna informazione trovata sulla crittografia dei dati inattiva».

Fase 6: Risolvi i risultati

Intervenite sui risultati che richiedono attenzione per migliorare il livello di sicurezza del vostro progetto.

Per i Non-compliantrisultati:

1. Consulta le linee guida consigliate per la riparazione.

2. Esamina qualsiasi documentazione interna collegata per un contesto aggiuntivo.
3. Aggiorna i documenti di progettazione per soddisfare i requisiti di sicurezza.
4. Documenta le modifiche apportate per riferimenti futuri.

Per risultati di dati insufficienti:

1. Leggi attentamente il commento per capire quali informazioni specifiche mancano.
2. Crea o aggiorna documenti di progettazione con i dettagli mancanti.
3. Prepara i file aggiornati per un nuovo invio.

Fasi successive

Dopo aver esaminato i risultati del progetto:

- Scarica il rapporto sui risultati come file CSV da condividere con il tuo team
- Aggiorna i documenti di progettazione per risolvere i risultati non conformi
- Crea documentazione aggiuntiva per i risultati insufficienti dei dati
- Condividi i risultati con il tuo team di sviluppo per discuterne
- Clona questa revisione del progetto per creare una nuova revisione con i documenti originali precaricati, in modo da aggiornare il nome ed eseguire nuovamente l'analisi per verificare i miglioramenti
- Procedi con l'implementazione per i progetti che soddisfano i requisiti di conformità

Per ulteriori informazioni sulla gestione dei requisiti di sicurezza, consultathe section called “Gestisci i requisiti di sicurezza”.

Per ulteriori informazioni sulla creazione di revisioni di progetti, consultathe section called “Crea una revisione del design”.

Crea un modello di minaccia

Crea modelli di minaccia nell'applicazione web AWS Security Agent per analizzare l'architettura dell'applicazione e identificare le minacce alla sicurezza. Un modello di minaccia produce due risultati principali: una panoramica del sistema che descrive come è costruito e si comporta il sistema e una

serie di minacce che descrive come il sistema potrebbe essere attaccato, ognuna con un livello di gravità, una classificazione STRIDE e raccomandazioni attuabili.

Un modello di minaccia accetta due tipi di input ed è possibile fornire uno o entrambi:

- Documenti relativi all'ambito: documenti tecnici di progettazione, specifiche delle API o documentazione sull'architettura che definiscono gli aspetti su cui si concentra il modello di minaccia. Quando viene fornita, l'agente elabora l'analisi in base al contesto descritto in questi documenti. Puoi caricare file (DOC, DOCX, JPEG, MD, PDF, PNG, TXT), fornire URI S3 o connettere pagine Confluence tramite un'integrazione.
- Sorgenti: codice sorgente proveniente da repository collegati (GitHub Enterprise Server o GitHub Bitbucket) o da sedi GitLab S3 GitLab Self-Managed. AWS Security Agent legge il codice sorgente per comprendere il sistema esistente. Se combinato con i documenti di ambito, il codice sorgente fornisce un contesto sull'implementazione corrente.

In questa procedura, si crea un modello di minaccia configurandone gli input e le autorizzazioni, quindi si avvia una corsa.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Accesso all'applicazione Web AWS Security Agent
- Almeno uno dei seguenti elementi:
  - Un repository connesso (GitHub GitHub Enterprise Server o Bitbucket) da utilizzare come sorgente (vedi) GitLab GitLab Self-Managed the section called “Abilita la modellazione delle minacce”
  - Un bucket S3 contenente codice sorgente
  - Progetta documenti da caricare come documenti di riferimento o come integrazione con Confluence

> **Tip**
>
> Se disponi già di repository o bucket S3 collegati a Agent Space (ad esempio, tramite la revisione del codice o la configurazione dei test di penetrazione), puoi creare immediatamente un modello di minaccia, senza richiedere alcuna configurazione aggiuntiva.

In che modo AWS Security Agent gestisce un modello di minaccia

Gli input forniti determinano il modo in cui AWS Security Agent esegue il modello di minaccia. Esistono tre scenari.

Input forniti	In che modo AWS Security Agent gestisce il modello di minaccia
Solo sorgenti (codice sorgente)	AWS Security Agent analizza il codice sorgente per comprendere la struttura dell'applicazione, classifica i componenti, estrae i flussi di dati, crea un modello di minaccia e identifica le minacce in base a come il sistema è effettivamente implementato.
Solo documenti Scope (documenti di progettazione)	AWS Security Agent esegue un modello di minaccia incentrato sul design descritto nei tuoi documenti. Identifica le minacce in base all'archi tettura, ai flussi di dati e ai componenti descritti nei documenti relativi all'ambito, utili per modellare le minacce di un progetto prima che esista qualsiasi codice.
Documenti relativi alle fonti e all'ambito	AWS Security Agent analizza il modello di minaccia in base al contesto descritto nei documenti dell'ambito (ad esempio, un documento di progettazione per una nuova funzionalità). Utilizza il codice sorgente per comprendere il sistema esistente, quindi modella le minacce in base al design descritto nei documenti relativi all'ambito, indipendentemente dal fatto che tale progetto sia già implementato o meno.

Accedi alla pagina dei modelli di minaccia

Vai alla sezione sulla modellazione delle minacce nell'applicazione web.

1. Accedi all'applicazione Web AWS Security Agent.
2. Nella barra laterale sinistra, scegli Threat models.
3. Viene visualizzato un elenco di modelli di minaccia esistenti con il relativo titolo, lo stato di esecuzione più recente e il numero di minacce per gravità.

Crea un modello di minaccia

Configura un nuovo modello di minaccia configurandone gli input e le autorizzazioni.

1. Nella pagina Modelli di minaccia, scegli Crea modello di minaccia.

Configura i dettagli del modello di minaccia

Fornisci un titolo per il tuo modello di minaccia.

1. Nel campo Titolo, inserisci un nome descrittivo per il tuo modello di minaccia.

> **Tip**
>
> Usa un nome che identifichi l'applicazione o il servizio da modellare. Ad esempio, «billing-service» o «checkout-api».

Aggiungi documenti Scope

Fornisci i documenti tecnici di progettazione che definiscono su cosa si concentra il modello di minaccia, come la documentazione sull'architettura, le specifiche delle API o le proposte di progettazione. Quando vengono forniti i documenti relativi all'ambito, l'agente elabora l'analisi in base al contesto descritto in questi documenti. I documenti relativi all'ambito sono facoltativi se si forniscono le fonti.

1. Nella sezione Documenti Scope, aggiungi documenti utilizzando uno o più dei seguenti metodi:
   - Carica file: carica direttamente i documenti di progettazione (DOC, DOCX, JPEG, MD, PDF, PNG o TXT).
   - URI S3: inserisci gli URI S3 che puntano ai documenti archiviati nei bucket S3 collegati.
   - Pagine Confluence: se disponi di un'integrazione Confluence connessa a Agent Space, seleziona le pagine dall'area di lavoro Confluence.

> **Tip**
>
> Per ottenere i migliori risultati, includi diagrammi di architettura, specifiche API e documentazione tecnica che descriva i componenti del sistema, i flussi di dati e i limiti di fiducia.

Aggiungi fonti

Seleziona il codice sorgente utilizzato da AWS Security Agent per comprendere il tuo sistema esistente. Se combinato con i documenti di ambito, il codice sorgente fornisce un contesto sull'implementazione corrente: l'agente lo utilizza per comprendere ciò che già esiste. Le fonti sono facoltative se si forniscono documenti di ambito.

1. Nella sezione Sorgenti, aggiungi il codice sorgente utilizzando uno o più dei seguenti metodi:

Archivi integrati

Seleziona tra i repository collegati al tuo Agent Space (GitHub GitHub Enterprise Server o GitLab Self-Managed Bitbucket). GitLab

1. Seleziona la casella di controllo accanto a ciascun repository che desideri includere come fonte.
2. Utilizza il campo di ricerca per trovare repository specifici per nome.

> **Note**
>
> Qui vengono visualizzati solo i repository collegati al tuo Agent Space. Per aggiungere altri repository, chiedi al tuo amministratore di aggiornare la configurazione di Agent Space.

Sorgenti S3

Aggiungi URI S3 che puntano al codice sorgente memorizzato nei bucket S3 collegati.

1. Inserisci l'URI S3 per ogni posizione del codice sorgente che desideri includere.

Configurazione delle risorse AWS

Seleziona il ruolo del servizio IAM e il gruppo di CloudWatch log opzionale per questo modello di minaccia.

1. Nel menu a discesa Service role, seleziona il ruolo IAM dai ruoli di servizio configurati.

> **Note**
>
> Il ruolo di servizio deve disporre delle autorizzazioni per accedere al codice sorgente in S3 e scrivere nei log. CloudWatch I ruoli di servizio vengono configurati durante la configurazione di Agent Space nella Console di gestione AWS.

2. (Facoltativo) Nel menu a discesa Log group, seleziona un gruppo di CloudWatch log per archiviare i log di esecuzione del modello di minaccia.

Crea il modello di minaccia

1. Verifica la configurazione.
2. Scegli Crea modello di minaccia.

Verrai reindirizzato alla pagina dei dettagli del modello di minaccia in cui puoi iniziare una corsa.

Esegui un modello di minaccia

Dopo aver creato un modello di minaccia, avvia un'esecuzione per iniziare l'analisi.

1. Nella pagina di dettaglio del modello di minaccia, scegli Avvia esecuzione.
2. AWS Security Agent inizia ad analizzare le fonti e i documenti relativi all'ambito.

Puoi anche avviare un'esecuzione dalla pagina di elenco dei modelli di minaccia selezionando Avvia esecuzione accanto al modello di minaccia che desideri eseguire.

Monitora l'esecuzione di un modello di minaccia

Tieni traccia dei progressi del tuo modello di minaccia man mano che viene eseguito.

Stato di esecuzione

L'intestazione della pagina di esecuzione mostra un indicatore di stato:

- In corso: l'agente del modello di minaccia è in esecuzione.
- Interruzione: è stato richiesto un annullamento; l'agente sta terminando l'attività corrente prima di interromperla.

- Completata: l'esecuzione è stata completata correttamente.
- Fallita: si è verificato un errore nell'esecuzione. Viene visualizzato un messaggio di errore con i dettagli. Inizia una nuova corsa dopo aver risolto il problema.
- Interrotta: l'esecuzione è stata annullata dall'utente. Tutte le minacce generate prima dell'interruzione vengono preservate.

Esegui le schede delle pagine

Nella pagina dei dettagli di esecuzione, naviga tra le schede:

- Panoramica: visualizza il riepilogo dell'esecuzione (ID del lavoro, ora di inizio, stato, durata) con un grafico a torta sui livelli di gravità che mostra la suddivisione delle minacce per gravità (critica, alta, media, bassa). Sotto il riepilogo, visualizza un grafico a barre delle categorie di minacce STRIDE che mostra quante minacce rientrano in ciascuna categoria STRIDE. Al termine dell'esecuzione, visualizza la panoramica del sistema prodotta dall'agente.
- Configurazione: visualizza le fonti, i documenti e le autorizzazioni (ruolo del servizio, gruppo di CloudWatch log) utilizzati per questa esecuzione.
- Preflight: visualizza lo stato dei controlli preliminari eseguiti prima dell'inizio dell'analisi delle minacce, inclusa la configurazione dell'infrastruttura di registrazione, la convalida dell'accesso alla sorgente S3 (se applicabile) e la configurazione dell'ambiente di test. Una barra di avanzamento mostra quanti controlli sono stati completati.
- Registri: visualizza un elenco filtrabile delle attività eseguite dall'agente durante l'esecuzione. Seleziona un'attività per visualizzarne l'output dettagliato del registro in un pannello laterale.
- Minacce: visualizza le minacce identificate durante l'esecuzione (vedithe section called “Esamina le minacce partendo da un modello di minaccia”).

Cronologia delle corse

Ogni modello di minaccia conserva una cronologia di tutte le esecuzioni. Nella pagina dei dettagli del modello di minaccia:

- La tabella delle esecuzioni elenca tutte le esecuzioni con ora di inizio, stato, durata, numero di minacce e ID.
- Scegli il link all'ora di inizio di una corsa per visualizzarne i dettagli completi.

> **Tip**
>
> Re-run lo stesso modello di minaccia dopo aver aggiornato il codice sorgente o modificato i documenti relativi all'ambito per vedere come la panoramica del sistema e le minacce cambiano nel tempo.

Modifica un modello di minaccia

Per modificare la configurazione del modello di minaccia:

1. Nella pagina dei dettagli del modello di minaccia, scegli Modifica.
2. Aggiorna il titolo, i sorgenti, i documenti di ambito o le risorse AWS secondo necessità.
3. Scegli Save changes (Salva modifiche).

> **Note**
>
> La modifica di un modello di minaccia non influisce sulle esecuzioni completate in precedenza. Questi conservano l'istantanea di configurazione utilizzata al momento dell'esecuzione.

Eliminare un modello di minaccia

Per eliminare un modello di minaccia e tutte le esecuzioni e le minacce associate:

1. Nella pagina di dettaglio del modello di minaccia, apri il menu delle azioni e scegli Elimina.
2. Conferma l'eliminazione.

> **Important**
>
> Se è attualmente in corso un'esecuzione, è necessario interromperla prima di eliminare il modello di minaccia.

Fasi successive

Dopo aver eseguito un modello di minaccia:

- Esamina la panoramica del sistema e le minacce (vedithe section called "Esamina le minacce partendo da un modello di minaccia")
- Re-run il modello di minaccia dopo aver apportato modifiche per verificare che le minacce siano state affrontate
- Modifica le fonti e l'ambito dei documenti man mano che l'applicazione si evolve

Esamina le minacce partendo da un modello di minaccia

Una volta completata l'esecuzione di un modello di minaccia, esamina la panoramica del sistema e le minacce per capire in che modo la tua applicazione potrebbe essere attaccata e cosa fare al riguardo. La panoramica del sistema è un documento completo che descrive l'architettura, i limiti di fiducia, i flussi di dati e il livello di sicurezza dell'applicazione. Ogni minaccia include una dichiarazione, il livello di gravità, la classificazione STRIDE, gli asset interessati e una raccomandazione per affrontarla.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Esecuzione completa del modello di minaccia
- Accesso all'applicazione Web AWS Security Agent

Fase 1: Accedere al modello di minaccia eseguito

Passa alla versione completa del modello di minaccia.

1. Accedi all'applicazione Web AWS Security Agent.
2. Nella barra laterale sinistra, scegli Threat models.
3. Seleziona il modello di minaccia che desideri esaminare.
4. Nella tabella delle esecuzioni, seleziona l'esecuzione completata scegliendo il relativo link all'ora di inizio.

Fase 2: Esamina la panoramica del sistema

La panoramica del sistema è una descrizione completa di come AWS Security Agent interpreta il tuo sistema. È un documento strutturato che può includere:

- Scopo: cosa fa il sistema e a chi serve.
- Funzionalità: funzionalità chiave fornite dal sistema.
- Intento progettuale: la modifica o la funzionalità di progettazione oggetto di un modello di minaccia (quando vengono forniti i documenti relativi all'ambito).
- Architettura: modalità di costruzione del sistema, inclusi modelli di implementazione e protocolli di comunicazione.
- Componenti: tabella dei componenti del sistema con il loro scopo e le interazioni chiave.
- Limiti di fiducia: dove cambiano i contesti di sicurezza, comprese le protezioni esistenti a ogni incrocio.
- Flussi di dati: descrizioni dettagliate del modo in cui i dati si spostano nel sistema, inclusi protocolli, credenziali e protezioni in ogni fase.
- Posizione di sicurezza: meccanismi attuali di autenticazione, crittografia e controllo degli accessi.
- Risorse sensibili: dati e credenziali che richiedono protezione, con relativa classificazione e punti di esposizione.
- Ipotesi chiave: Security-relevant ipotesi formulate dall'agente sul sistema.

Per visualizzare la panoramica del sistema:

1. Seleziona la scheda Panoramica.
2. Consulta la sezione di riepilogo dell'esecuzione, che mostra l'ID del lavoro, l'ora di inizio, lo stato e la durata.
3. Consulta il grafico del livello di gravità, che mostra una suddivisione delle minacce per gravità (critica, alta, media, bassa) con conteggi e percentuali.
4. Consulta il grafico delle categorie di minacce, che mostra quante minacce rientrano in ciascuna categoria STRIDE (spoofing, manomissione, ripudio, divulgazione di informazioni, negazione del servizio, elevazione dei privilegi).
5. Nella sezione Panoramica del sistema, leggi l'analisi completa dell'agente.

> **Tip**
>
> Se la panoramica del sistema non riflette fedelmente il sistema, perfeziona gli input, aggiungi gli archivi pertinenti come fonti o carica documenti più completi ed esegui nuovamente il modello di minaccia.

Fase 3: Analizza le minacce

Vai alla scheda Minacce per visualizzare tutte le minacce identificate durante l'esecuzione.

1. Seleziona la scheda Minacce.
2. Le minacce vengono visualizzate come un elenco con ogni scheda che riporta il titolo della minaccia, il badge di gravità, lo stato e il timestamp dell'ultimo aggiornamento. Puoi filtrare le minacce per gravità, stato o cercare per titolo.
3. Seleziona una minaccia dall'elenco per visualizzarne tutti i dettagli nel pannello a destra.

Gravità delle minacce

A ogni minaccia viene assegnato un livello di gravità:

- Critico: richiede un'azione immediata; lo sfruttamento potrebbe portare a una completa compromissione del sistema.
- Alto: richiede un'attenzione immediata; lo sfruttamento potrebbe avere un impatto significativo sulla sicurezza.
- Medio: deve essere affrontato in un lasso di tempo ragionevole; contribuisce al rischio complessivo per la sicurezza.
- Basso: può essere risolto nell'ambito di una manutenzione regolare; rischio immediato minimo.

Dettagli sulla minaccia

Seleziona una minaccia per visualizzarne i dettagli nel pannello a destra. I dettagli sono organizzati nelle seguenti sezioni:

Riga di metadati:

- Severità: il livello di rischio assegnato dall'agente (critico, alto, medio o basso).

- Categorie STRIDE: classificazione delle minacce: falsificazione, manomissione, ripudio, divulgazione di informazioni, negazione del servizio o elevazione dei privilegi.
- Creato il: quando la minaccia è stata identificata.
- Ultimo aggiornamento: data dell'ultima modifica della minaccia.

Sezione descrittiva:

- Dichiarazione: descrizione in linguaggio naturale della minaccia: cosa può fare la fonte della minaccia, qual è l'impatto e quali condizioni lo consentono.
- Fonte: l'attore o l'origine della minaccia (ad esempio, «utente autenticato» o «aggressore esterno»).
- Azione: cosa può fare la fonte della minaccia (ad esempio, «inserire query SQL nel parametro di ricerca»).
- Impatto: la diretta conseguenza dell'azione di minaccia (ad esempio, «accesso non autorizzato ai record dei clienti»).

Sezione Riferimenti:

- Risorse interessate: risorse specifiche interessate dalla minaccia (ad esempio, «record dei pagamenti dei clienti» o «tabella DynamoDB»).
- Prerequisiti: condizioni che devono essere soddisfatte affinché la minaccia sia sfruttabile.
- Obiettivi interessati: obiettivi di sicurezza interessati: riservatezza, integrità, disponibilità, autorizzazione, autenticazione o. Non-repudiation
- Evidenza: percorsi dei file del codice sorgente che supportano la minaccia, che rimandano a file specifici presenti nel repository.
- Anchor: un riferimento al codice che collega la minaccia a un nodo specifico del codice sorgente.

Sezione relativa ai consigli:

- Raccomandazione: guida pratica per affrontare la minaccia.

Fase 4: Creare una minaccia manualmente

È possibile aggiungere minacce che l'agente non ha identificato, ad esempio minacce scoperte durante la revisione manuale o provenienti da fonti esterne.

1. Nella scheda Minacce di un'esecuzione completata, scegli Crea minaccia.
2. Inserisci i dettagli della minaccia:
   - Dichiarazione: una descrizione della minaccia in linguaggio naturale.
   - Gravità: seleziona Critica, Alta, Media o Bassa.
   - Fonte: l'attore o l'origine della minaccia.
   - Prerequisiti: condizioni necessarie affinché la minaccia sia sfruttabile.
   - Azione: cosa può fare la fonte della minaccia.
   - Impatto: la diretta conseguenza dell'azione di minaccia.
   - Risorse interessate: risorse specifiche interessate (separate da virgole).
   - Obiettivi di sicurezza impattati: scegli tra Riservatezza, Integrità, Disponibilità, Autorizzazione, Autenticazione o. Non-repudiation
   - Categorie STRIDE: seleziona le categorie applicabili.
   - Raccomandazione: guida per affrontare la minaccia.
3. Scegli Create (Crea).

La minaccia creata manualmente appare nell'elenco delle minacce insieme alle minacce generate dall'agente.

Fase 5: Modifica e classifica le minacce

Mentre esamini le minacce, puoi modificarne i dettagli e aggiornarne lo stato per tenere traccia dei progressi.

1. Seleziona una minaccia dall'elenco.
2. Scegli l'icona di modifica nel pannello dei dettagli della minaccia per aprire il modulo di modifica.
3. È possibile modificare i seguenti campi:
   - Stato: monitora il ciclo di vita delle minacce:
     - Aperta: la minaccia viene riconosciuta e richiede attenzione (impostazione predefinita).
     - Risolto: il problema è stato risolto.
     - Ignorata: hai esaminato la minaccia e hai stabilito che non è applicabile.
   - Severità: modifica il livello di gravità se la valutazione dell'agente non corrisponde al tuo contesto.
   - Dichiarazione: perfeziona la descrizione della minaccia.

- Fonte, prerequisiti, azione, impatto: aggiorna i dettagli della minaccia in base alla conoscenza del dominio.
- Risorse interessate: aggiungi o rimuovi le risorse interessate (separate da virgole).
- Obiettivi di sicurezza interessati: seleziona gli obiettivi di sicurezza interessati (riservatezza, integrità, disponibilità, autorizzazione, autenticazione,). Non-repudiation

4. Scegli Salva per applicare le modifiche.

Passaggio 6: scaricare un rapporto

Al termine dell'esecuzione, puoi scaricare un rapporto PDF che riassume la panoramica del sistema e tutte le minacce identificate.

1. Nella pagina di esecuzione completata, scegli Genera rapporto.
2. Il PDF viene scaricato sul tuo computer.

Fase 7: Esaminare i controlli e i registri preliminari

Se avete bisogno di scoprire in che modo l'agente è giunto alle sue conclusioni o eseguire il debug di un errore parziale:

1. Seleziona la scheda Preflight per visualizzare lo stato dei controlli di preflight eseguiti prima dell'inizio dell'analisi delle minacce. Ogni controllo mostra il relativo stato (completo, in corso o in sospeso) e una barra di avanzamento indica quanti controlli sono stati completati. È possibile espandere un controllo completato per visualizzarne l'output dettagliato del registro.
2. Seleziona la scheda Registri per visualizzare un elenco filtrabile delle attività eseguite dall'agente durante l'esecuzione. Seleziona un'attività dall'elenco per visualizzarne l'output dettagliato del registro nel pannello laterale.

Fasi successive

Dopo aver esaminato i risultati del modello di minaccia:

- Affronta innanzitutto le minacce ad alta gravità sulla base delle raccomandazioni dell'agente
- Aggiorna gli stati delle minacce man mano che implementi le correzioni
- Esegui un nuovo modello di minaccia per verificare che le modifiche apportate rispondano alle minacce identificate

- Modifica le fonti e l'ambito dei documenti man mano che l'applicazione si evolve (vedi) the section called "Crea un modello di minaccia"

Esamina i risultati sulla sicurezza del codice nelle richieste pull

Dopo aver abilitato la revisione del codice per le pull request per i tuoi repository, AWS Security Agent analizza automaticamente le pull request e pubblica i risultati di sicurezza direttamente nel tuo provider di controllo del codice sorgente. Ciò consente agli sviluppatori di risolvere i problemi di sicurezza all'interno del loro normale flusso di lavoro senza uscire dalla pull request.

> **Note**
>
> Questa pagina si applica alle richieste GitHub pull, alle richieste di GitLab unione e alle richieste pull di Bitbucket. L'esperienza è simile per tutti i provider.

Come funziona la revisione del codice nelle pull request

Quando invii una pull request (o merge request GitLab) in un repository con la revisione del codice abilitata, AWS Security Agent avvia automaticamente l'analisi.

1. Trigger di analisi della pull request: la revisione del codice viene attivata quando una pull request viene contrassegnata come «Pronta per la revisione» nei repository in cui hai abilitato la funzionalità di revisione del codice. Le bozze di pull request non vengono analizzate.
2. Riconoscimento dell'analisi: quando AWS Security Agent inizia ad analizzare la richiesta pull, pubblica un commento iniziale: «AWS Security Agent sta analizzando il tuo codice...» Questo ti informa che l'analisi è iniziata ed è in corso.
3. Completamento della revisione: una volta completata l'analisi, AWS Security Agent pubblica una recensione sulla pull request con i risultati. Tutti i risultati di sicurezza vengono raggruppati in un'unica revisione per mantenere organizzata la pull request e ridurre al minimo le notifiche.

Comprensione dei risultati della revisione del codice

AWS Security Agent fornisce diversi tipi di risultati a seconda di ciò che trova durante l'analisi.

Quando vengono rilevati problemi di sicurezza

Se AWS Security Agent identifica problemi di sicurezza nelle modifiche al codice, pubblica una recensione che include:

- Riepilogo: una panoramica di alto livello di tutti i risultati di sicurezza, che descrive i tipi di problemi identificati e il loro potenziale impatto
- Risultati individuali: i risultati di sicurezza dettagliati vengono visualizzati sotto forma di commenti articolati nella parte inferiore della revisione principale, e ogni risultato include:
  - Descrizione del problema di sicurezza
  - Ubicazione nel codice in cui è stato rilevato il problema
  - Guida alla risoluzione che spiega come risolvere il problema
  - Contesto pertinente in base alle impostazioni di revisione del codice (violazioni dei requisiti di sicurezza, vulnerabilità comuni o entrambi)

> **Note**
>
> I tipi di problemi di sicurezza analizzati dipendono dalle impostazioni di revisione del codice. Se hai configurato la convalida dei requisiti di sicurezza, i risultati faranno riferimento ai requisiti di sicurezza personalizzati della tua organizzazione. Se hai configurato i risultati delle vulnerabilità di sicurezza, i risultati identificheranno le vulnerabilità di sicurezza più comuni. Per ulteriori informazioni sulle impostazioni di revisione del codice, consulta. the section called “Abilita la revisione del codice pull request per i GitHub repository”

Quando non vengono rilevati problemi di sicurezza

Se AWS Security Agent completa l'analisi e non rileva problemi di sicurezza nelle modifiche al codice, pubblica un commento: «Nessun problema identificato». Ciò conferma che la revisione è stata completata correttamente e che le modifiche al codice non hanno generato alcun problema di sicurezza in base alle impostazioni di revisione del codice configurate.

Risposta ai risultati di sicurezza

Dopo aver esaminato i risultati di sicurezza pubblicati da AWS Security Agent, puoi intervenire direttamente nel tuo provider di controllo del codice sorgente.

- Risolvi i risultati: aggiorna il codice in base alle linee guida di correzione fornite nei risultati, quindi invia nuovi commit alla pull request. AWS Security Agent analizzerà il codice aggiornato.
- Risolvi le conversazioni: dopo aver risolto un problema di sicurezza, contrassegna la conversazione come risolta per tenere traccia dei progressi.

> **Tip**
>
> Ogni risultato include linee guida specifiche per la risoluzione, personalizzate in base al problema di sicurezza identificato. Consulta attentamente questa guida per comprendere i rischi per la sicurezza e come affrontarli in modo efficace.

Filtraggio dei risultati della revisione del codice

Puoi personalizzare il modo in cui AWS Security Agent analizza il codice aggiungendo un `filtering.md` file al tuo repository. Questo file consente di ridurre i falsi positivi fornendo un contesto sulla base di codice ed escludendo file o cartelle dall'analisi.

Creazione del file di filtraggio

Crea un file denominato `filtering.md` nella `.awssecurityagent` directory alla radice del tuo repository:

```
.awssecurityagent/filtering.md
```

AWS Security Agent legge questo file dal ramo principale del repository (ad esempio, `main` o`mainline`) durante l'analisi delle richieste pull.

Struttura dei file

Il `filtering.md` file utilizza la formattazione Markdown standard con sezioni specifiche riconosciute da AWS Security Agent. Il file deve includere un'`Code Review`intestazione seguita da una o entrambe le seguenti sezioni: `IgnorePatterns` e `ContextHints` (senza spazio).

L'esempio seguente mostra la struttura completa di un `filtering.md` file:

```
# filtering.md
```

```
## Code Review

### IgnorePatterns

**/*.md

/myapp/src/**/*.snap

/myapp/config/README

### ContextHints

- The backend is a trusted system and won't return non-standard protocols.
- URL is generated from server with presigned token, so no SSRF security
 vulnerabilities.
- AppSec has verified that we are allowed to use cache with an eviction policy.
```

Ignora i modelli

La `IgnorePatterns` sezione specifica i file e le cartelle che AWS Security Agent deve ignorare durante la revisione del codice. `glob patterns`Utilizzato per definire quali percorsi escludere dall'analisi.

Requisiti di formato:

- Ogni modello deve essere su una riga distinta.
- Separa ogni motivo con una riga vuota tra di essi. Ciò garantisce il corretto rendering del file quando viene visualizzato nei nostri strumenti GitHub di revisione del codice.
- I pattern seguono il formato glob standard. Ad esempio, `**/*.md` corrisponde a tutti i file markdown e `/myapp/src/**/*.snap` corrisponde a tutti `.snap` i file all'interno della `/myapp/src/` cartella alla radice.
- In questa sezione supportiamo fino a 1000 modelli di ignoramento.

Suggerimenti contestuali

La `ContextHints` sezione fornisce un contesto aggiuntivo sulla tua base di codice che aiuta AWS Security Agent a effettuare valutazioni più accurate. Utilizza i suggerimenti di contesto per spiegare le decisioni architettoniche, le eccezioni di sicurezza o altre informazioni che potrebbero influire sul modo in cui i risultati vengono interpretati.

Requisiti di formato:

- Ogni suggerimento deve iniziare con un trattino (-) seguito da uno spazio.
- Scrivi ogni suggerimento come una singola riga di testo in formato libero limitata a 500 caratteri.
- Ogni suggerimento dovrebbe descrivere un contesto specifico sulla tua base di codice.
- In questa sezione supportiamo fino a 20 suggerimenti di contesto.

I suggerimenti di contesto vengono applicati dopo che AWS Security Agent ha completato l'analisi iniziale, aiutando a filtrare i risultati che non si applicano al caso d'uso specifico.

Fasi successive

Dopo aver esaminato i risultati sulla sicurezza del codice:

- Aggiorna il codice in base alle linee guida per la correzione
- Invia nuovi commit per avviare una nuova analisi delle modifiche
- Se necessario, modificate le impostazioni di revisione del codice (vedi) the section called "Abilita la revisione del codice pull request per i GitHub repository"
- Rivedi i requisiti di sicurezza della tua organizzazione per comprendere i criteri di convalida
- Prendi in considerazione i test di penetrazione per una convalida di sicurezza completa delle applicazioni distribuite

Creare una revisione del codice

Crea revisioni del codice nell'applicazione Web AWS Security Agent per scansionare i tuoi repository di codice sorgente e le fonti S3 alla ricerca di vulnerabilità di sicurezza. Le revisioni del codice eseguono un'analisi statica completa su tutta la base di codice, identificando i problemi di sicurezza e fornendo linee guida per la risoluzione.

A differenza della revisione del codice basata sulle pull request, che analizza le singole modifiche al codice (vedithe section called "Esamina i risultati sulla sicurezza del codice nelle richieste pull"), le revisioni del codice su richiesta scansionano l'intero codice sorgente per identificare le vulnerabilità di sicurezza e convalidare la conformità ai requisiti di sicurezza dell'organizzazione.

In questa procedura, creerai una revisione del codice selezionando gli input del codice sorgente, configurando le autorizzazioni ed eseguendo la revisione.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Accesso all'applicazione Web AWS Security Agent
- Almeno un GitHub repository o un bucket S3 connesso nel tuo Agent Space

> **Tip**
>
> Se disponi già di GitHub repository collegati a Agent Space, la revisione del codice è pronta per l'uso: non è richiesta alcuna configurazione aggiuntiva. Scegli Avvia nell'app web dalla scheda di revisione del codice nella pagina di Agent Space o avvia direttamente l'applicazione web.
> Se devi connettere fonti aggiuntive o configurare i bucket S3, consulta. the section called "Abilita la revisione del codice"

Accedi alla pagina di revisione del codice

Vai alla sezione delle revisioni del codice nell'applicazione web.

1. Accedi all'applicazione Web AWS Security Agent.
2. Nella barra laterale sinistra, scegli Code reviews.
3. Viene visualizzato un elenco di revisioni del codice esistenti con le informazioni sulla fonte, lo stato dell'ultima esecuzione e il riepilogo dei risultati.

Crea una revisione del codice

Imposta una nuova revisione del codice configurandone gli input e le autorizzazioni del codice sorgente.

1. Nella pagina di revisione del codice, scegli Crea revisione del codice.

Configura i dettagli della revisione del codice

Fornisci un titolo e seleziona il codice sorgente da esaminare.

1. Nel campo Titolo, inserisci un nome descrittivo per la revisione del codice.

> **Tip**
>
> Usa un nome che identifichi l'applicazione, l'archivio o l'ambito della revisione. Ad esempio, «billing-service-security-review» o «infrastructure-code-audit».

2. Nella sezione Sorgenti, seleziona gli input del codice sorgente per questa recensione. Scegliete tra due schede:

GitHub archivi

Seleziona tra i repository collegati al tuo Agent Space.

1. Scegli la scheda dei GitHub repository.
2. Nella tabella Archivi integrati, seleziona la casella di controllo accanto a ciascun repository che desideri includere nella revisione.
3. Utilizza il campo di ricerca per trovare repository specifici per nome.

> **Note**
>
> Qui vengono visualizzati solo i repository collegati a Agent Space tramite la configurazione di revisione del codice. Per aggiungere altri repository, scegli Gestisci nella console di amministrazione o chiedi all'amministratore di aggiornare la configurazione di Agent Space.

Sorgenti S3

Seleziona i file ZIP dai bucket S3 collegati al tuo Agent Space. L'amministratore di Agent Space configura quali bucket S3 sono disponibili. Qualsiasi file ZIP archiviato in uno di questi bucket può essere utilizzato come fonte per una revisione del codice.

1. Scegli la scheda Sorgenti S3.
2. Inserisci l'URI S3 di ogni file ZIP che desideri includere nella recensione. Puoi aggiungere fino a 30 sorgenti S3.

> **Note**
>
> Le fonti S3 devono essere file ZIP archiviati in bucket S3 collegati a Agent Space. Per rendere disponibili bucket aggiuntivi, consulta. the section called "Abilita la revisione del codice"

Configurazione delle autorizzazioni

Seleziona il ruolo del servizio IAM e il gruppo di CloudWatch log opzionale per questa revisione del codice.

1. Nella sezione Autorizzazioni, individua il menu a discesa del ruolo di servizio.
2. Seleziona il ruolo IAM dai ruoli di servizio configurati.

> **Note**
>
> Il ruolo di servizio deve disporre delle autorizzazioni per accedere al codice sorgente in S3 e scrivere nei CloudWatch log e qualsiasi altra risorsa AWS necessaria per la revisione del codice. I ruoli di servizio vengono configurati durante la configurazione della revisione del codice nella Console di gestione AWS.

3. (Facoltativo) Nel menu a discesa del gruppo di CloudWatch log, seleziona un gruppo di log per archiviare i log di esecuzione della revisione del codice.

> **Note**
>
> Se non si seleziona un gruppo di log, AWS Security Agent crea un gruppo di log predefinito per archiviare i log di revisione del codice.

Configura la correzione automatica del codice

Abilita la correzione automatica per consentire ad AWS Security Agent di generare correzioni di codice per tutti i risultati non appena la revisione è completata.

1. Nella sezione Correzione automatica del codice, seleziona la casella di controllo Abilita la correzione automatica del codice.

Il modo in cui AWS Security Agent fornisce la correzione dipende dalla fonte:

- GitHub Archivi privati: AWS Security Agent invia una pull request con la correzione al repository.
- GitHub Archivi pubblici: per evitare di rivelare la vulnerabilità prima che venga risolta, AWS Security Agent non apre una pull request. Allega invece una differenza suggerita alla scoperta che puoi scaricare dall'applicazione Web e candidarti privatamente.
- Sorgenti S3: la correzione del codice non è disponibile. Esamina i dettagli dei risultati e applica le correzioni manualmente.

> **Important**
>
> Le richieste di ripristino inviate agli archivi privati sono visibili a tutti coloro che dispongono dell'accesso in lettura. Rivedi le modifiche prima di procedere all'unione. La correzione automatica del codice è disponibile solo quando i GitHub repository sono selezionati come origine.

> **Note**
>
> Se disattivata, è comunque possibile attivare manualmente la correzione del codice per GitHub-sourced i singoli risultati dopo il completamento della revisione.

Configura la convalida simulata

Abilita la convalida simulata per confermare dinamicamente se le vulnerabilità scoperte sono sfruttabili in un'applicazione in esecuzione.

1. Nella sezione Convalida simulata, seleziona la casella di controllo Abilita convalida simulata.

Se abilitato, AWS Security Agent effettua il provisioning di un ambiente simulato dopo il completamento dell'analisi statica. Incorpora il codice sorgente, avvia i servizi all'interno dell'ambiente e tenta di sfruttare le vulnerabilità rilevate durante la scansione. I risultati vengono quindi aggiornati con uno stato di convalida che indica se la vulnerabilità è stata sfruttata con successo.

> **Note**
>
> La convalida simulata è attualmente disponibile solo per le applicazioni dockerabili autonome. Quando vengono selezionati più repository come fonti, la convalida simulata non è disponibile.

> **Important**
>
> La convalida simulata aggiunge tempo di elaborazione all'esecuzione della revisione del codice. La fase di convalida fornisce un ambiente ed esegue tentativi di sfruttamento. Questa operazione richiede in genere da 1 a 3 ore a seconda del numero di risultati e della complessità dell'applicazione.

Destinazioni di rete consentite

L'ambiente simulato ha un accesso alla rete in uscita limitato a una lista di autorizzazioni predefinita. L'applicazione può raggiungere i seguenti domini durante la convalida:

La tabella seguente elenca i domini consentiti e i relativi scopi.

Dominio	Scopo
`.amazonaws.com` , `.aws.amazon.com`	Servizi AWS
`.public.ecr.aws`	Amazon ECR Public
`.docker.com` , `.docker.io`	Docker Hub
`.github.com` , `.githubusercontent.com`	GitHub
`.gitlab.com`	GitLab
`.npmjs.com` , `.npmjs.org`	registro npm

Dominio	Scopo
`.pypi.org` , `.pypi.python.org` , `.pythonhosted.org`	Indice dei pacchetti Python
`.crates.io` , `.rustup.rs`	Pacchetti Rust
`.maven.org` , `.gradle.org`	Java/Gradle pacchetti
`.nuget.org`	pacchetti.NET
`.rubygems.org` , `.ruby-lang.org`	Pacchetti Ruby
`.golang.org` , `.pkg.go.dev` , `.goproxy.io`	Pacchetti Go
`.nodejs.org` , `.yarnpkg.com`	Node.js
`.alpinelinux.org` , `.debian.org` , `.ubuntu.com` , `.centos.org` , `.fedoraproject.org`	Repository di distribuzione Linux
`.cloudfront.net`	CloudFront distribuzioni
`.google.com` , `.googleapis.com`	API di Google
`.microsoft.com` , `.visualstudio.com`	Servizi Microsoft
`.sourceforge.net` , `.bitbucket.org`	Hosting dei sorgenti

> **Note**
>
> Se l'applicazione richiede l'accesso alla rete a domini non presenti in questo elenco, la connessione verrà bloccata dal firewall di rete. Le applicazioni che dipendono da API o servizi esterni non elencati sopra potrebbero non avviarsi correttamente nell'ambiente simulato.

Crea la revisione del codice

1. Rivedi la configurazione per garantirne l'accuratezza.
2. Scegli Crea revisione del codice.

Verrai reindirizzato alla pagina dei dettagli della revisione del codice dove puoi iniziare una revisione.

Esegui una revisione del codice

Dopo aver creato una revisione del codice, avvia un'esecuzione per iniziare l'analisi.

1. Nella pagina dei dettagli della revisione del codice, scegli Inizia revisione.
2. AWS Security Agent inizia ad analizzare il codice sorgente.

Puoi anche iniziare una revisione dalla pagina dell'elenco delle revisioni del codice selezionando Inizia revisione accanto alla revisione del codice che desideri eseguire.

Monitora l'esecuzione di una revisione del codice

Tieni traccia dello stato di avanzamento della revisione del codice durante l'esecuzione.

Rivedi le fasi di esecuzione

Un'esecuzione di revisione del codice procede attraverso le seguenti fasi, visualizzate come indicatore di avanzamento:

1. Preflight: AWS Security Agent convalida l'accesso al codice sorgente e configura l'ambiente di test. I controlli preliminari includono:
   - Configurazione dell'infrastruttura di servizio
   - Convalida dell'accesso alla sorgente S3
   - Configurazione dell'ambiente di test

2. Analisi statica: AWS Security Agent scansiona il codice sorgente alla ricerca di vulnerabilità di sicurezza e violazioni dei requisiti.
3. Convalida simulata (opzionale): se la convalida simulata è abilitata, AWS Security Agent fornisce un ambiente simulato e distribuisce l'applicazione. Quindi tenta di sfruttare le vulnerabilità scoperte durante l'analisi statica. Questo passaggio conferma se i risultati sono sfruttabili nel runtime di destinazione. Questa fase viene visualizzata solo quando si abilita la convalida simulata durante la creazione della revisione del codice.
4. Finalizzazione: AWS Security Agent compila i risultati e genera il riepilogo dei risultati.

Visualizza i dettagli della corsa

Nella pagina dei dettagli della corsa, naviga tra le schede per monitorare l'avanzamento:

- Esecuzione di revisione del codice: visualizza il riepilogo dell'esecuzione, che include l'ID di esecuzione, l'ora di creazione, lo stato, la durata, le ore dell'attività, la suddivisione del livello di gravità e il grafico dei tipi di rischio.
- Preflight: visualizza l'avanzamento e lo stato del controllo preliminare di ogni fase di convalida.
- Registri di revisione del codice: visualizza le attività che AWS Security Agent ha identificato e svolto durante la revisione, con log delle attività dettagliati per ogni fase.
- Convalida simulata: quando la convalida simulata è abilitata, visualizza lo stato del provisioning, le attività di convalida per i singoli risultati e i relativi risultati.
- Risultati: visualizza i risultati di sicurezza al termine della revisione (vedi). the section called "Esamina i risultati di una revisione del codice"

Esegui la cronologia

Ogni revisione del codice mantiene una cronologia di tutte le esecuzioni. Nella pagina dei dettagli della revisione del codice:

- La sezione Ultima esecuzione mostra l'esecuzione più recente con l'ora di inizio, lo stato, la durata e l'ID.
- La tabella Tutte le esecuzioni elenca tutte le esecuzioni precedenti con ora di inizio, stato, durata, riepilogo dei risultati e ID.
- Scegli Monitor run per visualizzare i dettagli dell'ultima esecuzione attiva.
- Scegli il link all'ora di inizio di una corsa per visualizzarne tutti i dettagli.

Fasi successive

Dopo aver eseguito una revisione del codice:

- Esamina i risultati di sicurezza e le relative linee guida per la correzione (vedithe section called "Esamina i risultati di una revisione del codice")
- Correggi i risultati tramite pull request automatizzate o correzioni manuali (vedi) the section called "Correggi i risultati della revisione del codice"
- Esegui ulteriori revisioni dopo aver implementato le correzioni per verificare la correzione
- Modifica la configurazione o le fonti di revisione del codice man mano che la tua codebase si evolve

Esamina i risultati di una revisione del codice

Al termine di un'esecuzione di revisione del codice, consulta il riepilogo dell'esecuzione e i risultati di sicurezza per comprendere le vulnerabilità del codice sorgente. Ogni risultato contiene una descrizione, un indice di gravità, le posizioni dei codici, un ragionamento dei rischi e le correzioni suggerite per aiutarti a stabilire le priorità e risolvere i problemi di sicurezza.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Un'esecuzione di revisione del codice completata o in corso
- Accesso all'applicazione Web AWS Security Agent

Fase 1: Accedere all'esecuzione di revisione del codice

Vai alla sessione di revisione del codice completata per visualizzare il riepilogo e i risultati.

1. Accedi all'applicazione web AWS Security Agent.
2. Nella barra laterale sinistra, scegli Code reviews.
3. Seleziona la revisione del codice che desideri esaminare.
4. Nella tabella Tutte le esecuzioni, seleziona l'esecuzione completata facendo clic sul relativo collegamento con l'ora di inizio. In alternativa, scegli Monitora l'esecuzione per visualizzare l'ultima esecuzione.

Passaggio 2: Monitora l'avanzamento della corsa

Tieni traccia dello stato di avanzamento dell'esecuzione della revisione del codice utilizzando l'indicatore dei passaggi.

1. Individua l'indicatore dei passaggi orizzontali sotto l'intestazione della pagina.
2. Esamina lo stato di ogni fase:
   - Preflight: convalida l'accesso al codice sorgente e configura l'ambiente di scansione. I controlli includono la configurazione dell'infrastruttura di servizio, la convalida dell'accesso alla sorgente S3 e la configurazione dell'ambiente di test, che include i controlli di accesso. GitHub
   - Analisi statica: analizza il codice sorgente alla ricerca di vulnerabilità di sicurezza e violazioni dei requisiti.
   - Convalida simulata (opzionale): se abilitata, effettua il provisioning di un ambiente simulato e tenta di sfruttare le vulnerabilità rilevate sull'applicazione in esecuzione.
   - Finalizzazione: compila i risultati e genera il riepilogo dei risultati.

> **Note**
>
> Ogni fase mostra un indicatore di stato (Completato o In corso). L'esecuzione è completa quando tutte le fasi mostrano Completato. La fase di convalida simulata viene visualizzata solo quando si abilita la convalida simulata durante la creazione della revisione del codice.

Fase 3: Rivedi il riepilogo dell'esecuzione

Vai alla scheda Code review run per visualizzare i risultati di alto livello.

1. Seleziona la scheda Code review run.
2. La sezione di riepilogo dell'esecuzione fornisce lo stato, la durata e altri dettagli di alto livello. Fornisce inoltre un pannello di controllo dei risultati di sicurezza classificati per livello di gravità e tipi di rischio.
3. La panoramica delle applicazioni fornita da AWS Security Agent fornisce un riepilogo della scansione di revisione del codice al termine dell'esecuzione

Fase 4: Esamina i risultati del test preliminare

Vai alla scheda Preflight per verificare che tutti i controlli di accesso alla fonte siano stati superati.

1. Seleziona la scheda Preflight.
2. Controlla l'indicatore di avanzamento di Preflight che mostra il numero di controlli completati.
3. Verifica che ogni controllo mostri uno stato di successo:
   - Configurazione dell'infrastruttura di servizio: conferma che l'ambiente di test è pronto
   - Convalida dell'accesso alla fonte S3: conferma l'accesso al codice sorgente S3 (se applicabile)
   - Ambiente di configurazione e test: conferma che l'ambiente di analisi è configurato

> **Note**
>
> Se un controllo di preflight fallisce, l'esecuzione non procederà all'analisi statica. Esamina i dettagli del controllo per identificare e risolvere i problemi di accesso, quindi avvia una nuova esecuzione.

Passaggio 5: Rivedi i registri di revisione del codice

Vai alla scheda Code review logs per visualizzare le attività eseguite da AWS Security Agent durante l'analisi.

1. Seleziona la scheda Code review logs.
2. Sfoglia l'elenco delle attività nel pannello di sinistra.
3. Seleziona un'attività per visualizzarne il registro dettagliato nel pannello di destra.

> **Tip**
>
> Utilizza il campo di ricerca per filtrare le attività per nome. I log forniscono informazioni su ciò che AWS Security Agent ha esaminato e su come è giunto alle sue conclusioni.

Fase 6: Passa ai risultati

Seleziona la scheda Risultati per visualizzare tutti i risultati relativi alla sicurezza durante l'esecuzione.

> **Note**
>
> Filtro di confidenza predefinito
>
> Per impostazione predefinita, vengono visualizzati solo i risultati con elevata confidenza degli agenti. Per mostrare anche i risultati con confidenza media o bassa degli agenti e i falsi positivi, disattiva l'opzione Nascondi i risultati non verificati.

1. Seleziona la scheda Risultati.
2. I risultati vengono visualizzati in una visualizzazione divisa con l'elenco dei risultati a sinistra e i dettagli del risultato selezionato a destra.
3. Controlla le informazioni visualizzate su ogni scheda di ricerca:
   - Titolo del reperto: un nome descrittivo che riassume il problema di sicurezza
   - Distintivo di gravità: indicatore di gravità: Color-coded
     - Critico (rosso): richiede un'azione immediata; lo sfruttamento potrebbe portare a una compromissione del sistema
     - Alto (rosso): richiede un'attenzione immediata; lo sfruttamento potrebbe avere un impatto significativo sulla sicurezza
     - Medio (arancione): deve essere affrontato in un lasso di tempo ragionevole; contribuisce al rischio complessivo per la sicurezza
     - Basso (giallo): può essere risolto nell'ambito di una manutenzione regolare; rischio immediato minimo
   - Ultimo aggiornamento: data e ora dell'ultimo aggiornamento del risultato

Fase 7: Rivedi i dettagli del ritrovamento

Seleziona i singoli risultati per visualizzare informazioni complete su ciascuna vulnerabilità.

1. Seleziona un risultato nel pannello di sinistra per visualizzarne i dettagli nel pannello di destra.
2. Esamina le azioni disponibili:

- Risolvi il problema: contrassegna il risultato come risolto dopo averlo risolto
- Codice correttivo: genera una pull request con una correzione (disponibile per i GitHub sorgenti)

3. Fornisci feedback utilizzando Questo risultato è stato accurato? — Seleziona Sì o No per migliorare la precisione delle analisi future.
4. Esamina gli attributi chiave nella sezione Panoramica:
   - Fiducia degli agenti: il livello di confidenza di AWS Security Agent in questo risultato
   - Severità: il livello di rischio con un badge codificato a colori
   - Tipo di rischio: la categoria di rischio per la sicurezza
   - Stato di convalida: quando la convalida simulata è abilitata, indica se il risultato è stato confermato sfruttabile in un ambiente in esecuzione:
     - Confermato: la vulnerabilità è stata sfruttata con successo nell'ambiente simulato
     - Non riprodotta: la vulnerabilità non può essere sfruttata nel runtime di destinazione
     - Convalida non riuscita: il tentativo di convalida non ha avuto esito positivo a causa di un errore
     - Non convalidato: la convalida simulata non è stata eseguita per questo risultato. Ciò si verifica quando la convalida non è abilitata o la fase di convalida è scaduta prima di raggiungere questo risultato.
   - Risolto: indica se il risultato è stato risolto () Yes/No
   - Ultimo aggiornamento: data e ora dell'aggiornamento più recente
5. Espandi la sezione Descrizione per leggere:
   - Una spiegazione dettagliata del problema di sicurezza
   - Come potrebbe essere sfruttata la vulnerabilità
   - Il potenziale impatto sulla tua applicazione
   - Fasi di verifica eseguite dall'agente per confermare il risultato
6. Espandi la sezione Posizioni dei codici per visualizzare:
   - Percorsi di file specifici in cui è stato identificato il problema
   - Una breve descrizione di ciò che è stato trovato in ciascuna località
   - Badge numerici di riga che rimandano al codice pertinente
7. Espandi la sezione Evidenze per esaminare:
   - Il codice, la configurazione o le osservazioni specifici che supportano la scoperta
   - Una breve spiegazione del motivo per cui ogni elemento dimostra la vulnerabilità
   - I file interessati e i numeri di riga per ogni elemento di prova

8. Espandi la sezione Correzione consigliata per visualizzare:
   - Le modifiche consigliate da AWS Security Agent per porre rimedio al risultato
   - Codice o configurazione di esempio per ogni modifica consigliata

> **Tip**
>
> Utilizza le posizioni del codice per accedere rapidamente ai file interessati nel tuo repository. Ogni posizione include un contesto sufficiente per comprendere il problema senza leggere l'intero file.

Fase 8: Assegnare priorità e risolvere i risultati

Convalida e agisci in base ai risultati per correggere le vulnerabilità e migliorare il livello di sicurezza dell'applicazione.

Per risultati di elevata gravità con elevata fiducia da parte degli agenti:

1. Esamina attentamente le sezioni Descrizione e Posizioni dei codici.
2. Usa il codice Remediate per generare una pull request con una correzione o rivedi i PR di riparazione automatici se hai abilitato questa opzione.
3. Pianifica un'ulteriore revisione del codice per verificare che la correzione sia efficace.

Per risultati di media gravità con elevata affidabilità da parte degli agenti:

1. Assegna le priorità in base alla tua propensione al rischio e al contesto aziendale.
2. Includi le attività di correzione nella normale pianificazione dello sprint di sviluppo.
3. Valuta se più risultati di media gravità insieme creino un rischio maggiore.

Per i risultati a media o bassa confidenza:

1. Consulta le sezioni Descrizione e Posizioni del codice per convalidare i presupposti e le condizioni in base ai quali si verifica la vulnerabilità.
2. Se la vulnerabilità è valida, stabilisci le priorità in base alla gravità e alla tolleranza al rischio e prendi in considerazione le attività di correzione.

Fase 9: Monitora l'avanzamento della riparazione

Utilizza l'interfaccia dei risultati e le ripetizioni per tenere traccia delle vulnerabilità risolte.

1. Durante l'implementazione delle correzioni, utilizza Resolve finding per contrassegnare i risultati come risolti.
2. Esegui una nuova revisione del codice per verificare che le correzioni risolvano i risultati e non introducano nuovi problemi.
3. Esamina la tabella Tutte le esecuzioni nella pagina dei dettagli di revisione del codice per confrontare i risultati tra le esecuzioni nel tempo.

> **Tip**
>
> Dopo aver unito le richieste pull di correzione, avvia una nuova esecuzione dello stesso codice per confermare che le vulnerabilità siano state risolte. Confronta il conteggio dei risultati tra le esecuzioni per monitorare i tuoi progressi.

Fasi successive

Dopo aver esaminato i risultati della revisione del codice:

- Dai priorità ai risultati di elevata gravità con elevata sicurezza per una correzione immediata
- Usa il codice Remediate per generare correzioni automatiche dei risultati (vedi) GitHub-sourced the section called “Correggi i risultati della revisione del codice”
- Esegui ulteriori revisioni del codice dopo aver implementato le correzioni per verificare la correzione
- Modifica le fonti o le impostazioni di revisione del codice man mano che la tua codebase si evolve (vedi) the section called “Abilita la revisione del codice”

Correggi i risultati della revisione del codice

Dopo aver esaminato i risultati di sicurezza derivanti da una revisione del codice, puoi utilizzare AWS Security Agent per generare correzioni di codice per i risultati nelle fonti del GitHub repository. Per i repository privati, AWS Security Agent apre una pull request con la correzione proposta. Per gli

archivi pubblici, AWS Security Agent allega al risultato una differenza scaricabile che puoi applicare localmente. I risultati provenienti da fonti S3 devono essere corretti manualmente.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Esecuzione di una revisione del codice completata con i risultati
- GitHub repository collegati come fonte per la revisione del codice
- Accesso all'applicazione Web AWS Security Agent
- Familiarità con l'architettura e i requisiti di sicurezza dell'applicazione

Come funziona la correzione del codice

Quando si attiva la correzione del codice per un risultato, AWS Security Agent analizza il risultato e le relative posizioni del codice, quindi genera una correzione del codice. Il modo in cui viene fornita la correzione dipende dalla fonte:

- GitHub Archivi privati: AWS Security Agent invia una pull request al repository pertinente. La pull request include una descrizione del problema di sicurezza e delle modifiche apportate.
- GitHub Archivi pubblici: AWS Security Agent associa una differenza suggerita al risultato in modo che la vulnerabilità non venga rivelata prima che venga risolta. Puoi scaricare il diff dall'applicazione Web e applicarlo localmente con. `git apply /path/to/code_remediation_changes.diff`
- Sorgenti S3: la correzione del codice non è disponibile. Utilizza la descrizione del risultato, le posizioni dei codici e il ragionamento dei rischi per applicare le correzioni manualmente.

> **Important**
>
> Le richieste pull create da AWS Security Agent sono visibili a tutti gli utenti che hanno accesso in lettura al repository. Rivedi le modifiche prima di unirle per assicurarti che siano in linea con i requisiti dell'applicazione.

Correzione automatica del codice

Se hai abilitato la correzione automatica del codice durante la creazione della revisione del codice, AWS Security Agent genera correzioni per tutti i risultati idonei non appena la revisione viene completata. Non è necessario intraprendere alcuna azione aggiuntiva: le pull request vengono visualizzate nei GitHub repository privati collegati e, man mano che l'esecuzione termina, compaiono differenze nei risultati degli GitHub archivi pubblici.

Correzione manuale del codice

Se la correzione automatica del codice è disattivata, è possibile attivare la correzione per singoli risultati dalle fonti. GitHub

1. Passa alla scheda Findings di un'esecuzione di revisione del codice completata.
2. Seleziona il risultato che desideri correggere.
3. Nel pannello dei dettagli del ritrovamento, scegli Correggi codice.
4. AWS Security Agent genera una correzione del codice e invia una richiesta pull al repository o allega una differenza scaricabile al risultato, a seconda della visibilità del repository.

Rivedi le richieste di ripristino

Dopo che AWS Security Agent ha inviato una richiesta di ripristino a un repository privato GitHub :

1. Accedi al tuo repository. GitHub
2. Individua la pull request creata da AWS Security Agent.
3. Rivedi le modifiche, tra cui:
   - La descrizione che spiega il problema di sicurezza e la correzione
   - Le modifiche al codice risolvono la vulnerabilità
   - Qualsiasi contesto rilevante relativo all'approccio correttivo
4. Unisci la pull request se la correzione è appropriata, oppure chiudila e implementa una soluzione alternativa.

> **Tip**
>
> Dopo aver unito le richieste pull di correzione, avvia una nuova esecuzione di revisione del codice per verificare che le correzioni risolvano i risultati e non introducano nuovi problemi di sicurezza.

Applica le differenze di correzione

Per i risultati provenienti da GitHub archivi pubblici, applica il diff scaricabile localmente.

1. Nel pannello dei dettagli del risultato, scarica il file diff dalla sezione Correzione del codice.
2. Nel clone locale del repository, esegui. `git apply /path/to/code_remediation_changes.diff`
3. Esaminate le modifiche applicate, testatele con la vostra applicazione e confermatele attraverso il normale flusso di lavoro di sviluppo.

Limitazioni

- La correzione del codice è disponibile solo per i risultati provenienti dalle fonti del GitHub repository. I risultati provenienti da fonti S3 devono essere corretti manualmente.
- AWS Security Agent genera correzioni basate sull'analisi della vulnerabilità. Rivedi tutte le modifiche prima di unirle o eseguirne il commit per assicurarti che siano appropriate per la tua applicazione.
- Alcuni risultati complessi possono richiedere un intervento manuale oltre alla correzione automatica.

Fasi successive

Dopo aver corretto i risultati:

- Esamina e unisci le richieste pull nei tuoi GitHub repository o conferma le differenze applicate attraverso il normale flusso di lavoro
- Esegui una nuova revisione del codice per verificare le correzioni e verificare i problemi rimanenti
- Risolvi i risultati nell'applicazione Web dopo aver confermato la correzione

- Modifica le fonti o le impostazioni di revisione del codice in base alle esigenze (vedi) the section called "Abilita la revisione del codice"

Esegui una scansione del codice differenziale con S3

Esegui una scansione del codice differenziale (diff) per analizzare solo le righe modificate nel codice sorgente, anziché eseguire una scansione completa del repository. Le scansioni differenziali sono più veloci delle scansioni complete e producono risultati mirati a modifiche specifiche del codice, il che le rende ideali per la convalida preliminare all'unione nei flussi di lavoro di sviluppo.

A differenza della revisione del codice basata su pull request, che viene attivata automaticamente dagli eventi dei provider di controllo del codice sorgente di terze parti (vedithe section called "Esamina i risultati sulla sicurezza del codice nelle richieste pull"), le scansioni differenziali vengono avviate a livello di codice tramite l'API o l'SDK di AWS Security Agent. Carichi un file diff unificato su S3 e vi fai riferimento quando inizi un processo di revisione del codice.

Come funzionano le scansioni differenziali

Una scansione differenziale analizza le modifiche al codice nell'intero contesto del repository. Quando crei una risorsa per la revisione del codice con il codice sorgente caricato su S3, la scansione differenziale utilizza l'intero repository come contesto, concentrando i risultati in modo specifico sulle righe modificate nel file diff. Ciò consente alla scansione di identificare i problemi di sicurezza derivanti dal modo in cui le modifiche interagiscono con il codice esistente, come flussi di autenticazione interrotti, gestione non sicura dei dati tra i moduli o modifiche che espongono le vulnerabilità esistenti.

Il processo di scansione:. Carichi un file diff unificato (l'output di`git diff`) in un bucket S3 collegato al tuo Agent Space. Chiami l'`StartCodeReviewJob`API con un `diffSource` parametro che punta alla posizione S3 del tuo diff. AWS Security Agent analizza solo il codice modificato nel file diff per verificare le vulnerabilità di sicurezza e la conformità ai requisiti di sicurezza dell'organizzazione. I risultati si riferiscono alle righe modificate, con livelli di gravità, posizioni dei codici e linee guida per la correzione.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Un Agent Space con revisione del codice abilitata (vedi) the section called "Abilita la revisione del codice"

- Una risorsa per la revisione del codice già creata per il repository di destinazione, con il codice sorgente completo caricato nel bucket S3 collegato all'Agent Space. L'archivio completo fornisce un contesto che consente un'analisi più approfondita del modo in cui le modifiche interagiscono con il codice esistente. Vedi the section called "Creare una revisione del codice" le istruzioni sulla creazione di una revisione del codice e sul caricamento del codice sorgente.
- Un bucket S3 collegato al tuo Agent Space
- Autorizzazioni IAM per il caricamento nel bucket S3 e la chiamata `securityagent:StartCodeReviewJob`
- Un file diff unificato generato dalle modifiche al codice (ad esempio, l'output di) `git diff main..feature-branch`

> **Tip**
>
> Per risultati più accurati, assicurati che la tua risorsa di revisione del codice abbia la versione più recente del codice sorgente completo caricata su S3. Il diff scan utilizza questo archivio completo come contesto per comprendere l'architettura dell'applicazione, i flussi di dati e i controlli di sicurezza esistenti durante l'analisi delle righe modificate.

Passaggio 1: generare un file diff

Genera un diff unificato che rappresenti le modifiche al codice che desideri scansionare.

```
git diff main..feature-branch > changes.diff
```

In alternativa, genera un diff per le modifiche graduali:

```
git diff --cached > changes.diff
```

> **Tip**
>
> Il file diff deve essere in formato diff unificato standard. AWS Security Agent analizza i percorsi dei file e le righe modificate dalle intestazioni diff per analizzarne l'analisi.

Passaggio 2: carica il file diff su S3

Carica il file diff in un bucket S3 collegato a Agent Space.

```
aws s3 cp changes.diff s3://my-security-agent-bucket/diffs/changes.diff
```

> **Important**
>
> Il bucket S3 deve essere già connesso al tuo Agent Space. Il ruolo di servizio IAM associato al tuo Agent Space deve avere accesso in lettura a questa posizione. Consulta the section called "Abilita la revisione del codice" le istruzioni su come collegare i bucket S3.

Fase 3: Inizia un lavoro di revisione del codice differenziale

Chiama l'`StartCodeReviewJob`API con il `diffSource` parametro per avviare una scansione differenziale.

Utilizzo della AWS CLI

```
aws securityagent start-code-review-job \
  --agent-space-id "your-agent-space-id" \
  --code-review-id "your-code-review-id" \
  --diff-source '{"s3Uri": "s3://my-security-agent-bucket/diffs/changes.diff"}'
```

Utilizzo dell'SDK AWS (Python)

```
import boto3

client = boto3.client('securityagent')

response = client.start_code_review_job(
    agentSpaceId='your-agent-space-id',
    codeReviewId='your-code-review-id',
    diffSource={
        's3Uri': 's3://my-security-agent-bucket/diffs/changes.diff'
    }
)

print(f"Job started: {response['codeReviewJobId']}")
```

Utilizzo dell'SDK AWS () JavaScript/TypeScript

```
import { SecurityAgentClient, StartCodeReviewJobCommand } from '@aws-sdk/client-
securityagent';

const client = new SecurityAgentClient({ region: 'us-east-1' });

const response = await client.send(new StartCodeReviewJobCommand({
  agentSpaceId: 'your-agent-space-id',
  codeReviewId: 'your-code-review-id',
  diffSource: {
    s3Uri: 's3://my-security-agent-bucket/diffs/changes.diff',
  },
}));

console.log(`Job started: ${response.codeReviewJobId}`);
```

L'API ritorna immediatamente con un `codeReviewJobId` and `status` of`IN_PROGRESS`.

Fase 4: Monitora la scansione

Esamina lo stato del lavoro di revisione del codice fino al suo completamento.

```
aws securityagent get-code-review-job \
  --agent-space-id "your-agent-space-id" \
  --code-review-id "your-code-review-id" \
  --code-review-job-id "the-job-id"
```

Il lavoro procede attraverso le stesse fasi di una revisione completa del codice: Preflight → Analisi statica → Finalizzazione. Le scansioni differenziali in genere vengono completate più velocemente delle scansioni complete perché analizzano meno righe di codice.

Fase 5: Esaminare i risultati

Una volta completato il lavoro, elenca i risultati del processo di revisione del codice.

```
aws securityagent list-findings \
  --agent-space-id "your-agent-space-id" \
  --code-review-id "your-code-review-id" \
  --code-review-job-id "the-job-id"
```

Ogni risultato include:

- Una descrizione del problema di sicurezza
- Il livello di gravità (critico, alto, medio o basso)
- Posizioni del codice che fanno riferimento a righe specifiche nel diff
- Ragionamento del rischio che spiega il potenziale impatto
- Linee guida per la riparazione

Per ulteriori informazioni su come comprendere e agire in base ai risultati, vederethe section called "Esamina i risultati di una revisione del codice".

Quote e limiti

- Numero massimo di file modificati in una differenza: 3.000 file o una dimensione totale del diff di 5 MB
- I risultati sono limitati a 30 per scansione, con priorità in base alla gravità (Critico > Alto > Medio > Basso)

Fasi successive

Dopo aver eseguito una scansione differenziale:

- Esamina i risultati e applica le linee guida per la correzione (vedi) the section called "Esamina i risultati di una revisione del codice"
- Abilita i commenti delle pull request per la revisione automatica del codice su ogni pull request (vedithe section called "Abilita la revisione del codice pull request per i GitHub repository")
- Eseguite periodicamente una revisione completa del codice per individuare eventuali problemi al di fuori delle singole modifiche (vedithe section called "Creare una revisione del codice")
- Utilizzate l'integrazione IDE per eseguire scansioni differenziali direttamente dal vostro ambiente di sviluppo (vedi) the section called "Esegui scansioni di sicurezza del codice dal tuo IDE"

Esegui scansioni di sicurezza del codice dal tuo IDE

Esegui scansioni di sicurezza del codice di AWS Security Agent direttamente dal tuo IDE utilizzando Kiro o Claude Code. L'integrazione IDE ti consente di scansionare il codice sorgente locale alla

ricerca di vulnerabilità di sicurezza, eseguire scansioni differenziali solo sul codice modificato ed eseguire revisioni dei modelli di minaccia sui documenti di progettazione, il tutto senza uscire dall'ambiente di sviluppo. I risultati vengono visualizzati insieme al codice con indicazioni sulla correzione e puoi applicare correzioni automatiche direttamente dall'IDE.

Come funziona l'integrazione IDE

L'integrazione IDE utilizza il server MCP (Model Context Protocol) di AWS Security Agent per connettere l'IDE al servizio AWS Security Agent:

1. Il server MCP impacchetta il codice sorgente in un archivio ZIP.
2. L'archivio viene caricato in un bucket S3 che il server esegue automaticamente il provisioning nel tuo account AWS.
3. Il server chiama l'API AWS Security Agent per avviare una scansione.
4. AWS Security Agent analizza il codice per individuare le vulnerabilità di sicurezza e la conformità ai requisiti di sicurezza dell'organizzazione.
5. I risultati vengono restituiti all'IDE con posizioni dei codici, descrizioni, valutazioni di gravità e suggerimenti di correzione.

Il server MCP gestisce tutta l'orchestrazione (provisioning dello spazio degli agenti, creazione di bucket S3, configurazione dei ruoli IAM, packaging del codice e scan polling), quindi sono necessarie solo le credenziali AWS configurate localmente.

> **Note**
>
> L'unico prerequisito sono le credenziali AWS configurate nell'ambiente locale (ad esempio, tramite `aws configure` AWS SSO o variabili di ambiente). Il server MCP effettua automaticamente il provisioning dell'Agent Space, del ruolo di servizio IAM e del bucket S3 al primo utilizzo.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Credenziali AWS configurate localmente con le seguenti autorizzazioni:

  - `iam:CreateRole`, `iam:PutRolePolicy` (per la configurazione una tantum del ruolo di servizio)
  - `s3:CreateBucket`, `s3:PutObject`, `s3:PutPublicAccessBlock`, `s3:PutLifecycleConfiguration`
  - `securityagent:CreateAgentSpace`, `securityagent:UpdateAgentSpace`, `securityagent:ListAgentSpaces`, `securityagent:BatchGetAgentSpaces`
  - `securityagent:CreateCodeReview`, `securityagent:StartCodeReviewJob`, `securityagent:BatchGetCodeReviewJobs`
  - `securityagent:ListFindings`, `securityagent:BatchGetFindings`
  - `securityagent:StartCodeRemediation`(per correzioni automatiche)
  - `sts:GetCallerIdentity`
- uv installato (gestore di pacchetti Python)
- Python 3.10 o successivo
- Uno dei seguenti IDE:
  - Kiro (installa AWS Security Agent Power)
  - Claude Code (installa il plug-in AWS Security Agent)

Installa il server MCP

Kiro

Installa AWS Security Agent Power dal marketplace Kiro. Power raggruppa la configurazione del server MCP, le istruzioni di guida e gli hook del ciclo di vita per suggerimenti automatici di scansione di sicurezza.

In alternativa, configura il server MCP manualmente nel tuo progetto: `.kiro/mcp.json`

```
{
  "mcpServers": {
    "security-agent": {
      "command": "uvx",
      "args": ["awslabs.security-agent-mcp-server@latest"],
      "env": {
        "AWS_PROFILE": "default",
        "AWS_REGION": "us-east-1",
        "FASTMCP_LOG_LEVEL": "ERROR"
```

```
      }
    }
  }
}
```

Codice Claude

Installa il plug-in AWS Security Agent, che fornisce competenze per la configurazione, le scansioni complete, le scansioni delle differenze, la revisione dei modelli di minaccia e la correzione.

Configura il server MCP nel tuo progetto: `.mcp.json`

```
{
  "mcpServers": {
    "awslabs.security-agent-mcp-server": {
      "command": "uvx",
      "args": ["awslabs.security-agent-mcp-server@latest"],
      "env": {
        "AWS_PROFILE": "default",
        "AWS_REGION": "us-east-1",
        "FASTMCP_LOG_LEVEL": "ERROR"
      }
    }
  }
}
```

> **Tip**
>
> Puoi anche eseguire il server MCP tramite Docker se preferisci non installare Python localmente. Consulta la documentazione del server MCP per la configurazione di Docker.

First-time configurazione

Al primo utilizzo, il server MCP effettua automaticamente il provisioning delle risorse AWS richieste:

Risorsa	Convenzione sui nomi	Scopo
Agent Space	User-chosen o creato automaticamente	Contenitore per scansioni, recensioni e pentest

Risorsa	Convenzione sui nomi	Scopo
Ruolo di servizio IAM	`SecurityAgentScanRole`	Presumuto `securityagent.amazonaws.com` per leggere il codice caricato
Bucket S3	`security-agent-scans-{account}-{region}`	Memorizza il codice sorgente compresso (ciclo di vita con scadenza automatica di 30 giorni)

Per attivare la configurazione in modo esplicito, chiedi al tuo IDE:

```
Set up the security agent
```

La configurazione verifica le credenziali AWS, crea o riutilizza un Agent Space, effettua il provisioning del ruolo IAM e del bucket S3 e conferma la disponibilità. Se disponi già di Agent Spaces dalla Console di gestione AWS, la configurazione li mostra e chiede quale usare.

> **Note**
>
> La configurazione viene eseguita automaticamente alla prima scansione se non è già configurata. Non è necessario eseguirlo separatamente.

Esegui una scansione di sicurezza completa

Scansiona l'intero progetto per individuare eventuali vulnerabilità di sicurezza:

```
Scan this project for security issues
```

L'IDE:

1. Archivia il codice sorgente (esclusi `.git` gli `node_modules` artefatti di compilazione e altre directory non essenziali)
2. Carica l'archivio su S3
3. Avvia un processo completo di revisione del codice

4. Sondaggi da completare (in genere circa 1 ora)
5. Presenta i risultati raggruppati per gravità

Avanzamento della scansione

Le scansioni complete richiedono in genere circa 1 ora a seconda della dimensione del codebase. L'IDE controlla i progressi ogni 5 minuti e ti avvisa quando i risultati sono pronti. Puoi richiedere lo stato in qualsiasi momento:

```
How's the scan going?
```

Esegui una scansione differenziale

Per un feedback più rapido durante lo sviluppo, scansiona solo il codice modificato dopo un git ref:

```
Scan my changes against main for security issues
```

Per impostazione predefinita, se non specifichi un riferimento di base, la scansione confronta le modifiche non salvate. `HEAD` Puoi specificare esplicitamente una base diversa:

```
Diff scan my uncommitted changes
```

Le scansioni differenziali caricano sia il contesto completo del repository che la patch git diff, quindi eseguono un'analisi focalizzata solo sulle righe modificate. I risultati in genere arrivano in 5-15 minuti.

Per ulteriori informazioni sull'API diff scan di S3, consulta. the section called "Esegui una scansione del codice differenziale con S3"

Esegui una revisione del modello di minaccia

Analizza i documenti di progettazione per verificare eventuali modifiche al livello di sicurezza utilizzando la metodologia STRIDE:

```
Run a threat model review on my spec
```

L'IDE identifica l'utente `requirements.md` e i `design.md` file (in genere sottostanti `.kiro/specs/`), li carica insieme al codice sorgente ed esegue un'analisi del modello di minaccia. I risultati identificano:

- Minacce alla sicurezza classificate da STRIDE (falsificazione, manomissione, ripudio, divulgazione di informazioni, negazione del servizio, elevazione dei privilegi)
- Classificazioni di gravità per ogni minaccia
- Impatto su risorse specifiche della tua codebase
- Raccomandazioni per la mitigazione

> **Tip**
>
> Esegui una revisione del modello di minaccia prima di generare attività di implementazione in base a una specifica. In questo modo vengono rilevati i problemi di progettazione della sicurezza prima che il codice venga scritto.

Esaminare i risultati

Al termine di una scansione, i risultati vengono visualizzati nell'IDE raggruppati per gravità:

```
# CRITICAL: SQL Injection in user-service.ts
   File: src/api/user-service.ts:45
   User input flows directly into SQL query without parameterization

# HIGH: Hardcoded credentials in config.ts
   File: src/config/database.ts:12
   Database password stored in source code
```

Viene inoltre redatto un rapporto dettagliato `.security-agent/findings-{scan_id}.md` con informazioni complete per ogni risultato, tra cui il tipo di rischio, il punteggio di confidenza, le posizioni dei codici e il codice di correzione.

Per visualizzare i risultati di una scansione precedente:

```
Show my security findings
```

Applica correzioni automatiche

Dopo aver esaminato i risultati, applica la correzione automatica:

```
Fix the security findings
```

L'IDE elabora i risultati dall'alto verso il basso per gravità (Critico → Alto → Medio → Basso), applicando le correzioni al codice utilizzando le linee guida per la correzione di ogni risultato. Dopo aver applicato tutte le correzioni, esegue automaticamente una scansione delle differenze di verifica per confermare che i problemi sono stati risolti.

Puoi anche correggere singoli risultati:

```
Fix the SQL injection in user-service.ts
```

> **Important**
>
> Controlla sempre le correzioni automatiche prima di eseguire il commit. Verifica che le correzioni non interrompano le funzionalità esistenti o introducano regressioni.

Suggerimenti di scansione automatica (Kiro)

Quando si utilizza Kiro Power, AWS Security Agent può suggerire automaticamente scansioni delle differenze dopo aver apportato modifiche al codice sensibili alla sicurezza. The Power installa un hook che valuta ogni turno di codifica completato e suggerisce una scansione quando le modifiche influiscono su:

- Logica di autenticazione o autorizzazione
- Crittografia o gestione dei segreti
- Convalida degli input o sanificazione dei dati
- Richieste di rete o integrazioni esterne
- Configurazione di sicurezza (CORS, intestazioni, gestione delle sessioni)

Puoi disattivare i suggerimenti automatici in qualsiasi momento eliminandoli. `.kiro/hooks/security-diff-scan-suggester.kiro.hook`

Tipi di scansione disponibili

Tipo di scansione	Durata	Caso d'uso	Comando
Scansione completa	Circa 1 ora	Revisione completa dell'intera base di codice	«Scansiona il mio progetto per individua re eventuali problemi di sicurezza»
Scansione Diff	5—15 minuti	Solo codice modificat o (pre-commit, pre-PR)	«Scansiona le mie modifiche» o «Scansione delle differenze rispetto alla versione principale»
Modello di minaccia	5—30 minuti	Documenti di progettazione (requirements.md, design.md)	«Esegui una revisione del modello di minaccia in base alle mie specifiche»

Variabili di ambiente

Variabile	Description	Predefinita
`AWS_REGION`	Regione AWS per le chiamate SecurityAgent API	`us-east-1`
`AWS_PROFILE`	Nome del profilo delle credenziali AWS	Profilo predefinito
`FASTMCP_LOG_LEVEL`	Livello di registro del server MCP (DEBUG, INFO, WARNING, ERROR)	`WARNING`

Risoluzione dei problemi

«Non configurato. Esegui prima la configurazione».

Il tuo `.security-agent/config.json` è scomparso o l'Agent Space non esiste più. Chiedi all'IDE di eseguire la configurazione:

```
Set up the security agent
```

La scansione fallisce con AccessDenied

Assicurati che le tue credenziali AWS abbiano le autorizzazioni IAM richieste elencate nella sezione Prerequisiti. L'autorizzazione mancante più comune è `iam:CreateRole` (necessaria solo per la prima configurazione).

La scansione scade o impiega troppo tempo

- Le scansioni complete su basi di codice di grandi dimensioni possono richiedere più di 1 ora
- Utilizza le scansioni differenziali per lo sviluppo iterativo: vengono completate in pochi minuti
- Verifica che l'archivio di origine non includa directory non necessarie (il server MCP esclude automaticamente gli schemi comuni)

Differenza vuota: nessuna modifica alla scansione

Se si esegue una scansione delle differenze senza modifiche non eseguite, il server MCP segnala «Nessuna modifica rispetto a HEAD» e non avvia una scansione. Conferma o organizza prima le modifiche oppure specifica un riferimento di base diverso.

Quote e limiti

- Dimensione massima dell'archivio sorgente: 2 GB
- Ciclo di vita del bucket S3: il codice caricato viene eliminato automaticamente dopo 30 giorni

Fasi successive

Dopo aver eseguito la prima scansione di sicurezza IDE:

- Abilita i commenti di revisione del codice pull request per GitHub l'integrazione automatizzata (vedithe section called “Abilita la revisione del codice pull request per i GitHub repository”)
- Configura i requisiti di sicurezza per la convalida delle politiche specifiche dell'organizzazione (vedi) the section called “Gestisci i requisiti di sicurezza”
- Esegui scansioni complete periodiche per individuare eventuali problemi nell'intera codebase (vedi) the section called “Creare una revisione del codice”
- Utilizza le revisioni dei modelli di minaccia sulle specifiche delle nuove funzionalità prima dell'implementazione

Crea un test di penetrazione

Imposta test di penetrazione automatizzati per le tue applicazioni Web configurando l'ambito del test, i domini di destinazione e l'accesso alle risorse AWS. I test di penetrazione aiutano a identificare le vulnerabilità di sicurezza nelle applicazioni in esecuzione simulando scenari di attacco reali contro i tuoi domini verificati.

AWS Security Agent esegue test di sicurezza completi sulle tue applicazioni Web in base all'ambito e alle autorizzazioni configurati, fornendo risultati dettagliati sulle vulnerabilità sfruttabili prima che gli aggressori possano scoprirle.

In questa procedura, creerai un test di penetrazione configurando i dettagli del test, definendo l'ambito del test e impostando le autorizzazioni richieste.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Accesso all'applicazione Web AWS Security Agent
- Almeno un dominio verificato per i test
- Ruolo IAM con autorizzazioni appropriate per AWS Security Agent
- Comprensione dell'architettura e dei percorsi critici dell'applicazione

Inizia a creare un test di penetrazione

Vai alla pagina di creazione del test di penetrazione nell'Agent Web App.

1. Accedi all'applicazione Web AWS Security Agent.
2. Vai alla sezione dei test di penetrazione.
3. Scegli Crea un test di penetrazione.

> **Tip**
>
> Nei test di penetrazione possono essere inclusi solo i domini verificati. Chiedi al tuo amministratore di verificare il dominio nella console di gestione AWS. Per informazioni, consulta the section called "Abilita un dominio applicativo per i test di penetrazione".

Dai un nome al tuo penetration test

Fornisci un nome descrittivo che aiuti a identificare lo scopo e l'ambito di questo penetration test.

1. Nel campo Nome del test di penetrazione, inserisci un nome descrittivo per il tuo test di penetrazione.

   Example

   Il nome deve identificare chiaramente l'applicazione, l'ambiente o il componente da testare. Massimo 100 caratteri.

Configura l'ambito del test di penetrazione

Definisci quali domini e percorsi URL verranno testati e configura esclusioni opzionali per controllare i limiti del test.

Aggiungi domini di destinazione

Specificate i domini verificati che verranno testati attivamente per rilevare eventuali vulnerabilità di sicurezza.

1. Nella sezione Ambito del test di penetrazione, individua gli URL di Target.
2. Espandi la sezione Domini verificati per visualizzare i domini disponibili.
3. Nel campo URL di destinazione, inserisci l'URL del dominio di destinazione.

> **Important**
>
> È possibile testare solo i domini verificati. L'URL deve appartenere a un dominio precedentemente verificato in AWS Security Agent. Sub-domains di un dominio verificato non è necessaria una verifica separata.

4. Per aggiungere più domini di destinazione:
   a. Scegli Add domain (Aggiungi dominio).
   b. Inserisci l'URL di ogni dominio aggiuntivo.
5. Per rimuovere un dominio di destinazione, scegli Rimuovi accanto all'URL del dominio.

> **Tip**
>
> Per ottenere risultati ottimali, includi tutti i domini che fanno parte del flusso di utenti dell'applicazione, inclusi i sottodomini per le API, i servizi di autenticazione e la distribuzione di contenuti. Sub-domains di un dominio principale verificato non è necessaria una verifica separata.

Escludi i tipi di rischio (opzionale)

Scegliete categorie di rischio specifiche da escludere dai test se non sono applicabili alla vostra applicazione.

1. Individua il campo Escludi i tipi di rischio.
2. Scegli il menu a discesa per visualizzare i tipi di rischio disponibili.
3. Seleziona uno o più tipi di rischio da escludere dal penetration test.

> **Note**
>
> L'esclusione dei tipi di rischio limita l'ambito del test. Escludi solo i tipi di rischio che non sono pertinenti alla tua applicazione o che desideri testare separatamente.

Aggiungi percorsi URL non compresi nell'ambito (opzionale)

Specificate i percorsi URL che non devono essere testati durante il penetration test. AWS Security Agent esclude il percorso specificato e tutti i percorsi annidati al di sotto di esso. Ad esempio, se lo aggiungi `https://example.com/admin` come URL non rientrante nell'ambito, lo è anch'esso. `https://example.com/admin/tools`

1. Out-of-scope Individua la sezione URL.
2. Nel campo di immissione degli Out-of-scope URL, inserisci un percorso URL da escludere (ad esempio `/admin/delete` o`/api/reset`).

> **Warning**
>
> Out-of-scope i percorsi non vengono testati per verificare la presenza di vulnerabilità. Assicurati di escludere solo i percorsi a cui non si dovrebbe accedere durante i test, come operazioni distruttive o funzioni amministrative sensibili.

3. Per aggiungere più percorsi non compresi nell'ambito:
   a. Scegli Aggiungi URL.
   b. Inserisci ogni percorso aggiuntivo.
4. Per rimuovere un percorso, scegli Rimuovi accanto al percorso.

Aggiungi domini accessibili (opzionale)

Specificate i domini necessari per il test ma che non sono obiettivi per i test di vulnerabilità.

1. Individua la sezione URL accessibili.
2. Nel campo di immissione URL accessibili, inserisci un dominio che dovrebbe essere accessibile durante il test.

> **Note**
>
> Aggiungi domini accessibili per servizi di terze parti (come Okta, Auth0, Stripe) esterni al dominio di destinazione. Ciò è necessario affinché AWS Security Agent possa accedere a questi URL per l'accesso e la navigazione durante i test. AWS Security Agent NON esegue test di penetrazione su questi domini: vengono utilizzati esclusivamente per scopi di accesso. I domini accessibili non richiedono la verifica della proprietà, anche se

appartengono a un dominio diverso da quello di destinazione. Solo i domini di destinazione richiedono una proprietà verificata.

3. Per aggiungere più domini accessibili:
   a. Scegli Aggiungi URL.
   b. Inserisci ogni dominio aggiuntivo.
4. Per rimuovere un dominio, scegli Rimuovi accanto al dominio.

Aggiungi intestazioni HTTP personalizzate (opzionale)

Specificare le intestazioni HTTP personalizzate che verranno aggiunte a qualsiasi richiesta effettuata da AWS Security Agent durante i test di penetrazione.

1. Individua la sezione Intestazioni HTTP personalizzate.
2. Nel campo di immissione delle intestazioni HTTP personalizzate, inserisci un nome e un valore di intestazione che verranno associati alle richieste in uscita.

> **Note**
>
> Per impostazione predefinita, AWS Security Agent aggiunge un'intestazione personalizzata da User-Agentimpostare su securityagent a meno che non venga specificato un valore di User-Agentintestazione personalizzato diverso.

3. Per aggiungere più intestazioni personalizzate:
   a. Seleziona Add header (Aggiungi intestazione).
   b. Inserisci ogni intestazione personalizzata aggiuntiva.
4. Per rimuovere un'intestazione personalizzata, scegli Rimuovi accanto all'intestazione.

Configura IAM Role

Seleziona il ruolo di servizio preconfigurato per questo test di penetrazione. AWS Security Agent utilizza un modello di Space-based autorizzazione degli agenti in cui gli amministratori configurano i ruoli IAM durante la configurazione di Agent Space. Puoi scegliere tra ruoli già configurati e pronti all'uso.

1. Nella sezione Autorizzazioni, individua il menu a discesa Ruoli di servizio.

2. Seleziona il ruolo IAM che concede ad AWS Security Agent l'accesso alle risorse AWS richieste.

> **Important**
>
> Il ruolo IAM selezionato deve disporre delle autorizzazioni per accedere alle risorse VPC CloudWatch , ai log e a qualsiasi altro servizio AWS necessario per il test di penetrazione. Verifica che il ruolo abbia la corretta relazione di fiducia con AWS Security Agent.

3. Individua il menu a discesa del gruppo di CloudWatch log.
4. Seleziona il gruppo di log in cui verranno archiviati i log dei test di penetrazione. (opzionale)

> **Note**
>
> Il gruppo di CloudWatch log selezionato memorizzerà i registri dettagliati dell'esecuzione del penetration test, incluse le richieste effettuate, le risposte ricevute e le vulnerabilità scoperte.
> Se non si seleziona un gruppo di log, verrà creato automaticamente un nuovo gruppo di CloudWatch log con il `/aws/securityagent` prefisso per memorizzare i log dei penetration test.

Correzione automatica del codice

Seleziona la casella di controllo Abilita la riparazione automatica.

> **Important**
>
> Per correggere i problemi di sicurezza nei tuoi repository di codice sorgente, AWS Security Agent può inviare richieste pull ai tuoi repository. Le pull request possono essere visibili a tutti gli utenti che hanno accesso in lettura ai repository.

Configurazione delle risorse VPC (opzionale)

Se i domini di destinazione sono privati e ospitati all'interno di un VPC, configura le impostazioni VPC in cui AWS Security Agent deve eseguire i test di penetrazione. Questo passaggio è necessario solo per le applicazioni che non sono accessibili al pubblico.

> **Note**
>
> Salta questo passaggio se i tuoi domini di destinazione sono accessibili pubblicamente. La configurazione VPC è richiesta solo per testare applicazioni private ospitate all'interno di un Amazon Virtual Private Cloud.

Scegli il VPC, le sottoreti e i gruppi di sicurezza per l'ambiente di test di penetrazione.

1. Nella sezione VPC, individua il menu a discesa VPC ID.
2. Seleziona il VPC in cui sono ospitati i tuoi domini di destinazione.

> **Important**
>
> Il VPC selezionato deve contenere i domini di destinazione specificati nel passaggio 3. Assicurati che il VPC abbia un routing e una configurazione di rete appropriati per consentire ad AWS Security Agent di accedere alle tue applicazioni.

3. Individua il menu a discesa Subnet.
4. Seleziona una o più sottoreti in cui eseguire il test di penetrazione.

> **Note**
>
> Scegliete sottoreti con accesso di rete alle applicazioni di destinazione. Il test di penetrazione verrà eseguito dalle risorse distribuite in queste sottoreti.

5. Individua il menu a discesa del gruppo di sicurezza.
6. Seleziona il gruppo di sicurezza che controlla l'accesso alla rete per il penetration test.

> **Important**
>
> Il gruppo di sicurezza selezionato deve consentire il traffico in uscita verso i domini di destinazione e tutti i domini accessibili. Assicurati che le regole del gruppo di sicurezza consentano l'accesso alla rete necessario per test completi.

Configura le credenziali di autenticazione (opzionale)

Se i domini di destinazione richiedono l'autenticazione, fornisci le credenziali per consentire ad AWS Security Agent di accedere alle aree protette dell'applicazione durante i test di penetrazione. Questo passaggio è necessario solo per le applicazioni che richiedono l'autenticazione dell'utente.

> **Note**
>
> Salta questo passaggio se i tuoi domini di destinazione non richiedono l'autenticazione o se tutte le aree che desideri testare sono accessibili al pubblico. Configura le credenziali solo quando hai bisogno di AWS Security Agent per testare le sezioni autenticate della tua applicazione.

Aggiunta di credenziali

Fornisci le credenziali di autenticazione che AWS Security Agent utilizzerà per accedere alla tua applicazione.

1. Nella sezione Credential #1, seleziona un metodo di immissione delle credenziali:
   - Credenziali di immissione: inserisci le tue credenziali direttamente in AWS Security Agent.
   - Impostazioni avanzate: per informazioni sensibili sulle credenziali, utilizza opzioni avanzate come AWS Secrets Manager o le funzioni AWS Lambda. Per informazioni dettagliate, vedi the section called "Fornisci credenziali di autenticazione per i test di penetrazione".

     > **Tip**
     >
     > Per ambienti di produzione o credenziali sensibili, consigliamo di utilizzare l'opzione di impostazione avanzata per fare riferimento in modo sicuro alle credenziali archiviate in AWS Secrets Manager o Systems Manager Parameter Store.

Inserisci i dettagli delle credenziali

Fornisci il nome utente e la password per l'account autenticato.

1. Nel campo Nome utente, inserisci il nome utente per l'autenticazione.
2. Nel campo Password, inserisci la password per l'autenticazione.

> **Important**
>
> Assicurati che le credenziali fornite abbiano livelli di accesso appropriati per le aree che desideri testare. Le credenziali devono rappresentare il livello di accesso di un utente tipico anziché i privilegi amministrativi.

Seleziona il dominio di accesso

Specificate quale dominio di destinazione utilizzerà queste credenziali per l'autenticazione.

1. Nel menu a discesa del dominio di accesso, seleziona il dominio in cui verranno utilizzate queste credenziali.

> **Note**
>
> Se disponi di più domini di destinazione che richiedono credenziali diverse, puoi aggiungere set di credenziali aggiuntivi facendo clic su Aggiungi un'altra credenziale dopo aver completato questa configurazione delle credenziali.

Configura la richiesta di accesso dell'agente (opzionale)

Fornisci istruzioni per guidare AWS Security Agent nel processo di autenticazione dell'applicazione.

1. Espandi la sezione relativa alla richiesta di accesso dell'agente se il flusso di autenticazione richiede istruzioni specifiche.
2. Inserisci le istruzioni che descrivono come utilizzare le credenziali fornite nel flusso di accesso dell'applicazione.

> **Note**
>
> La richiesta di accesso dell'agente indica all'agente come applicare le credenziali all'applicazione. Ciò è utile per flussi di autenticazione complessi, processi di accesso in più fasi o applicazioni con procedure di accesso non standard. Includi istruzioni dettagliate come «Vai a /login, inserisci il nome utente nel campo 'Email', inserisci la password e scegli 'Accedi'».

Aggiungi più credenziali (opzionale)

Se l'applicazione richiede più set di credenziali o domini diversi richiedono un'autenticazione separata, aggiungi altri set di credenziali.

1. Dopo aver completato la prima configurazione delle credenziali, scegli Aggiungi un'altra credenziale.
2. Ripeti i passaggi di configurazione delle credenziali per ogni set di credenziali aggiuntivo.
3. Per rimuovere un set di credenziali, scegli Rimuovi accanto all'intestazione delle credenziali.

> **Tip**
>
> Configura più credenziali durante il test di diversi ruoli utente, l'accesso a più domini autenticati o la verifica dei controlli di accesso basati sui ruoli nell'applicazione.

Allega risorse aggiuntive (opzionale)

Fornisci risorse supplementari per aiutare AWS Security Agent a condurre test di penetrazione più completi e accurati. Le risorse aggiuntive possono includere diagrammi di architettura, documentazione API, file di configurazione, GitHub repository o S3-hosted materiali che forniscono un contesto sull'applicazione.

> **Note**
>
> Le risorse aggiuntive sono facoltative ma consigliate. Fornire informazioni complete sull'applicazione aiuta a garantire una copertura completa dei test, riduce i falsi positivi e fornisce risultati più utilizzabili.

Aggiungi risorse al test di penetrazione

Seleziona le risorse esistenti o carica nuovi file che ti aiuteranno a guidare il test di penetrazione.

1. Nella sezione Risorse connesse, puoi:
   - Scegli Seleziona tra disponibili per scegliere tra le risorse già connesse ad AWS Security Agent (come GitHub repository o bucket S3).

- Scegli Carica per aggiungere nuovi file direttamente dal tuo sistema locale.

> **Tip**
>
> Le risorse utili includono documentazione sulle API, diagrammi di architettura, OpenAPI/Swagger specifiche, file di configurazione, diagrammi di flusso di autenticazione e qualsiasi altro materiale che descriva la struttura e il comportamento dell'applicazione.

Seleziona tra le risorse disponibili

Scegli tra risorse già integrate con AWS Security Agent.

1. Scegli Select tra le risorse esistenti.
2. Sfoglia l'elenco delle risorse disponibili da fonti connesse come:
   - GitHub repository, nella scheda GitHub repository
   - Bucket S3
   - File caricati in precedenza
   - Archivi di documentazione
3. Seleziona le risorse che desideri includere nel test di penetrazione.
4. Scegli Aggiungi al test di penetrazione per allegare le risorse selezionate.

Example

Ti consigliamo di selezionare e aggiungere GitHub repository pertinenti al tuo pentest, in modo che AWS Security Agent possa sviluppare una comprensione del contesto dell'applicazione e generare correzioni di codice pronte per l'implementazione tramite pull request (se abilitate)

> **Note**
>
> Le risorse selezionate tra le fonti disponibili rimangono sincronizzate con la loro posizione originale. Se aggiorni un GitHub repository o un file S3, il penetration test utilizzerà la versione aggiornata.

> **Note**
>
> Se hai un VPC privato associato al tuo pentest e un GitHub repository configurato, assicurati che GitHub sia accessibile tramite il tuo VPC privato per estrarre risorse. GitHub Nella maggior parte dei casi, dovrai assicurarti che il traffico in uscita tramite VPC NAT Gateway sia consentito per impostazione predefinita o configurare regole specifiche per consentire il traffico in uscita GitHub per gli IP (GitHub vedi Meta API Endpoint)

Carica nuove risorse

Carica i file direttamente dal tuo sistema locale o fornisci contenuti in testo semplice ad AWS Security Agent.

1. Scegli Carica.
2. Scegli uno dei seguenti metodi di input:
   - Carica file locali: seleziona uno o più file dal tuo sistema locale.
   - Incolla testo semplice: digita o incolla il contenuto del testo direttamente nel campo di immissione. Scegli Carica.
3. Quindi scegli Aggiungi per completare il caricamento.
4. Le risorse caricate vengono visualizzate nella tabella Risorse connesse.

> **Tip**
>
> Utilizza l'opzione di testo semplice quando desideri fornire rapidamente elenchi di endpoint API, modelli di URL, istruzioni di test o altre informazioni basate su testo senza creare un file separato.

> **Important**
>
> Assicurati che i file caricati e i contenuti incollati non contengano informazioni sensibili come credenziali di produzione, chiavi private o informazioni di identificazione personale (PII). Utilizza versioni igienizzate dei file di configurazione e della documentazione.

Connect le risorse esistenti

Le risorse esistenti possono provenire da ciò che hai precedentemente caricato su AWS Security Agent, dal tuo bucket S3 e dai tuoi repository integrati GitHub . Scegli Seleziona tra le risorse esistenti per selezionarle.

Gestisci le risorse connesse

Rivedi, organizza e rimuovi le risorse allegate al test di penetrazione.

La tabella Risorse connesse mostra tutte le risorse incluse nel test di penetrazione con le seguenti informazioni:

- Nome: il nome del file o l'identificatore della risorsa
- Tipo: la categoria di risorse (file caricati, risorse S3, GitHub repository, ecc.)

Per gestire le risorse:

1. Seleziona una o più risorse utilizzando le caselle di controllo.
2. Scegli Rimuovi dal test di penetrazione per scollegare le risorse selezionate.

> **Note**
>
> Puoi ordinare la tabella per nome o tipo facendo clic sulle intestazioni delle colonne. Questo aiuta a organizzare le risorse quando si lavora con molti file.

Crea il test di penetrazione

Finalizza e avvia la configurazione del test di penetrazione.

Dopo aver configurato tutte le impostazioni, sei pronto per creare il penetration test.

1. Rivedi tutte le sezioni di configurazione per garantire la precisione.
2. Scegli una delle seguenti opzioni:
   - Scegli Create penetration per salvare la configurazione senza eseguirla immediatamente.
   - Scegli Crea ed esegui per salvare la configurazione e avviare immediatamente il test di penetrazione.

- Scegli Annulla per eliminare la configurazione del test di penetrazione.

> **Important**
>
> Prima di eseguire un test di penetrazione, verificate che:
>
> - Tutti i domini di destinazione sono verificati e accessibili correttamente
> - I ruoli IAM dispongono delle autorizzazioni appropriate
> - Out-of-scope i percorsi sono configurati correttamente per impedire il test di operazioni distruttive
> - Hai l'autorizzazione a eseguire test di sicurezza su tutti i domini di destinazione

> **Note**
>
> Dopo l'inizio del test di penetrazione, puoi monitorarne l'avanzamento dalla sezione Esecuzioni dei test di penetrazione. Il completamento del test può richiedere diverse ore. Il più completo entro 16 ore, a seconda dell'ambito e della complessità della domanda.

Esamina i risultati di un test di penetrazione

Monitora l'esecuzione del pentest in tempo reale nella pagina Penetration Test Logs dopo che AWS Security Agent ha avviato un pentest. AWS Security Agent registra ogni azione durante il pentest. Al termine, consulta il riepilogo del pentest, che include una panoramica delle applicazioni, la copertura con gli endpoint identificati e la valutazione del rischio dei risultati di sicurezza.

Valuta i risultati di sicurezza per risolvere le vulnerabilità delle applicazioni. Ogni risultato contiene la valutazione dell'impatto, la valutazione della gravità, le prove di supporto e i dettagli delle pull request di correzione (quando è abilitata la correzione automatica del codice).

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Un test di penetrazione completato o in corso
- Accesso all'applicazione Web AWS Security Agent

Fase 1: Accedere all'esecuzione del test di penetrazione

Vai al test di penetrazione per visualizzare le pagine di panoramica, i log e i risultati.

1. Accedi all'applicazione web AWS Security Agent.
2. Vai alla sezione dei test di penetrazione.
3. Seleziona l'esecuzione del test di penetrazione che desideri esaminare dall'elenco.

> **Tip**
>
> La pagina dei dettagli del penetration test mostra un riepilogo dello stato del test, della data di completamento e del numero di risultati identificati.

Fase 2: Monitora l'avanzamento del test

Tieni traccia dei progressi del tuo test di penetrazione utilizzando l'indicatore dei passaggi.

1. Individua l'indicatore dei passaggi orizzontali sotto l'intestazione della pagina.
2. Esamina lo stato di ogni fase di test:
   - Preflight: configurazione iniziale e controlli della connettività
   - Analisi statica: analisi del codice e della configurazione
   - Pentests: test di runtime e scansione delle vulnerabilità
   - Finalizzazione: convalida finale e generazione di report

> **Note**
>
> Ogni passaggio mostra un indicatore di stato (Completo, In corso o In sospeso). I risultati vengono scoperti e convalidati durante tutto il processo di test, con la comparsa di nuove vulnerabilità al termine di ogni fase.

Passaggio 3: vai alla scheda panoramica sull'esecuzione del test di penetrazione

1. La sezione Run Summary fornisce lo stato, la durata e altri dettagli di alto livello del test. Fornisce inoltre una dashboard dei risultati di sicurezza classificati per livello di gravità e tipi di rischio

2. La panoramica delle applicazioni di AWS Security Agent fornisce un riepilogo del penetration test eseguito
3. Discovered endpoints by AWS Security Agent fornisce un elenco di tutti gli endpoint scoperti e testati dall'agente di sicurezza AWS durante l'esecuzione del pentest.

Passaggio 4: accedi alla scheda dei log dei test di penetrazione

Accedi ai log dettagliati di tutte le azioni eseguite da AWS Security Agent durante il pentest.

1. Le azioni sono classificate per tipo di azione e tipi di rischio.
2. Seleziona un'azione specifica per visualizzare i log dettagliati:
   - Riepilogo dei test: High-level riepilogo delle azioni e dei risultati dell'agente
   - Registri dei test di penetrazione: registri dettagliati di tutte le attività di test

> **Note**
>
> Le azioni di validazione forniscono registri che convalidano i risultati in ogni categoria

> **Note**
>
> La scheda Risultati mostra una visualizzazione divisa con l'elenco dei risultati a sinistra e i dettagli dei risultati selezionati a destra.

Passaggio 5: vai ai risultati

Ogni risultato dell'elenco mostra informazioni chiave per aiutarti a valutarne rapidamente l'importanza.

> **Note**
>
> Filtro di confidenza predefinito
>
> Per impostazione predefinita, vengono visualizzati solo i risultati con elevata confidenza degli agenti. Per mostrare anche i risultati con confidenza media o bassa degli agenti e i falsi positivi, disattiva l'opzione Nascondi i risultati non verificati.

Controlla le informazioni visualizzate su ogni scheda di ricerca:

- Nome del ritrovamento: il titolo e l'identificatore della vulnerabilità
- Distintivo di confidenza: indica il livello di fiducia dell'agente nel risultato (alto, medio o basso)
- Distintivo di severità: mostra il livello di rischio con la codifica a colori:
  - Critico (rosso): richiede un'azione immediata; lo sfruttamento potrebbe comportare una compromissione del sistema
  - Alto (rosso): richiede un'attenzione immediata; lo sfruttamento potrebbe avere un impatto significativo sulla sicurezza
  - Medio (arancione): deve essere affrontato in un lasso di tempo ragionevole; contribuisce al rischio complessivo per la sicurezza
  - Basso (giallo): può essere risolto nell'ambito di una manutenzione regolare; rischio immediato minimo
  - Informativo (blu): a scopo informativo; rischio immediato minimo o nullo
- Data e ora dell'ultimo aggiornamento: mostra quando il risultato è stato modificato o convalidato l'ultima volta
- Anteprima della descrizione: breve riepilogo della vulnerabilità

> **Important**
>
> Assegna priorità ai risultati con badge di gravità critica o elevata e livelli di confidenza elevati, poiché rappresentano vulnerabilità convalidate che richiedono una correzione immediata.

Fase 6: Rivedi i dettagli del ritrovamento

Seleziona i singoli risultati per visualizzare informazioni complete su ciascuna vulnerabilità.

1. Seleziona il nome di un risultato nel pannello di sinistra per visualizzarne i dettagli nel pannello di destra.
2. Verifica lo stato di convalida:

> **Note**
>
> Se in un risultato viene visualizzato lo Sconosciuto «Questo risultato non è ancora stato convalidato da AWS Security Agent», significa che il rilevamento della vulnerabilità è ancora in fase di conferma. Questi risultati possono richiedere una verifica manuale.

3. Esamina gli attributi chiave visualizzati in alto:
   - Fiducia degli agenti: il livello di confidenza di AWS Security Agent in questo risultato
   - Severità: il livello di rischio con un badge codificato a colori
   - Ricerca dei log: scegli «Trace actions & logs» per visualizzare i log di esecuzione dettagliati e le prove
   - Tipo di rischio: la categoria o il tipo di rischio per la sicurezza (ad esempio Authentication Bypass, SQL Injection)
4. Espandi la sezione Descrizione per leggere:
   - Una spiegazione dettagliata della vulnerabilità
   - Come funziona la vulnerabilità
   - Perché rappresenta un rischio per la sicurezza
   - Il potenziale impatto sulla tua applicazione
5. Espandi la sezione Risk Reasoning per comprendere il calcolo della gravità:
   - Analisi delle metriche CVSS (Common Vulnerability Scoring System)
   - Attack Vector (AV): come sfruttare la vulnerabilità
   - Complessità dell'attacco (AC): quanto è difficile l'exploit
   - Privilegi richiesti (PR): quale livello di accesso è necessario
   - Interazione con l'utente (UI): se è richiesta l'azione dell'utente
   - Ambito (S): se la vulnerabilità riguarda altri componenti
   - Impatti su riservatezza, integrità e disponibilità
6. Espandi la sezione Passaggi per la riproduzione per visualizzare:
   - Procedure tecniche dettagliate per ricreare la vulnerabilità
   - Esempi di richieste e risposte
   - Parametri o condizioni specifici che determinano il problema
7. La sezione Script di verifica fornisce un modo eseguibile per riprodurre il risultato. Espandi questa sezione (se disponibile) per visualizzare:

- Istruzioni: come configurare ed eseguire lo script di verifica
- Variabili di ambiente: elenca le variabili obbligatorie da configurare prima di eseguire lo script. I valori sensibili vengono oscurati per motivi di sicurezza.
- Scarica script: scegli di scaricare lo script di verifica eseguibile

> **Note**
>
> Gli script di verifica sono disponibili solo per le vulnerabilità confermate. L'agente deve aver generato e convalidato correttamente uno script di riproduzione eseguibile.

> **Note**
>
> Gli script di verifica vengono generati utilizzando l'intelligenza artificiale generativa. Esamina lo script prima dell'esecuzione ed eseguilo solo su sistemi che sei autorizzato a testare. Per indicazioni su come testare AI-generated gli script in modo responsabile, consulta la policy AWS Responsible AI.

> **Tip**
>
> Lo script di verifica fornisce un modo eseguibile per riprodurre i risultati in modo indipendente. Imposta le variabili di ambiente richieste con le tue credenziali, quindi esegui lo script sul sistema di destinazione per confermare l'esistenza della vulnerabilità.

> **Tip**
>
> Utilizza il link «Trace actions & logs» per accedere al pacchetto di prove completo, comprese le richieste HTTP, le risposte e i tentativi di sfruttamento che dimostrano la vulnerabilità.

Modifica i risultati

Puoi modificare qualsiasi risultato per correggerne i dettagli o affinare la valutazione dell'agente. I seguenti campi sono modificabili:

- name: il titolo del risultato
- descrizione: descrizione dettagliata della vulnerabilità di sicurezza
- status: stato attuale del risultato
- RiskType: tipo di rischio per la sicurezza identificato
- Livello di rischio: livello di gravità (CRITICO, ALTO, MEDIO, BASSO, INFORMATIVO)
- RiskScore: punteggio di rischio numerico
- ragionamento: giustificazione del punteggio di rischio assegnato
- AttackScript: Proof-of-concept codice che dimostra la vulnerabilità
- CustomerNote: nota facoltativa che spiega le motivazioni alla base della modifica

Per modificare un risultato:

1. Vai alla pagina dei dettagli del risultato.
2. Scegli l'icona di modifica per modificare uno qualsiasi dei campi nell'elenco precedente.
3. Salvare le modifiche.

> **Note**
>
> Le modifiche vengono salvate immediatamente e riportate nei risultati. Se la personalizzazione dei risultati è abilitata, tutti i campi modificabili modificati verranno utilizzati per affinare le preferenze dell'agente per le esecuzioni future.

Visualizza la versione originale dell'agente

Quando modificate un risultato, nell'intestazione dei dettagli del risultato viene visualizzato un selettore di versione. Ciò consente di visualizzare la valutazione originale dell'agente:

1. Individua il selettore di versione nell'intestazione dei dettagli di ricerca.
2. Seleziona Originale per visualizzare il risultato così com'è stato originariamente prodotto dall'agente.
3. Seleziona Più recente per tornare alla versione corrente con le modifiche applicate.

Rivedi i risultati personalizzati

Quando Findings Personalization è abilitata, AWS Security Agent apprende dalle modifiche apportate ai risultati. L'agente applica tali preferenze a risultati simili nelle future esecuzioni dei test di penetrazione. Quando un risultato è stato modificato in base alle modifiche precedenti, il pannello dei dettagli mostra una sezione Modifiche alla personalizzazione. Per informazioni sull'attivazione di questa funzionalità, consulta Abilitare o disabilitare la personalizzazione dei risultati.

1. Individua la sezione Modifiche alla personalizzazione nel pannello dei dettagli della ricerca.

> **Note**
>
> La sezione Modifiche alla personalizzazione viene visualizzata solo sui risultati che AWS Security Agent ha allineato alle modifiche precedenti. I risultati che non corrispondono alle preferenze acquisite vengono mostrati esattamente come li ha prodotti l'agente, senza questa sezione.

2. Consulta il riepilogo di cosa è cambiato e perché. Il riepilogo elenca ogni attributo modificato con il valore originale prodotto dall'agente, il valore personalizzato e il ragionamento. Ad esempio:

In base alle modifiche precedenti, sono state apportate le seguenti modifiche ai risultati originariamente prodotti dal sistema: il livello di rischio è passato da MEDIO a CRITICO; il punteggio di rischio è cambiato da 5,3 a 9,5; Motivazione: la severità è stata aggiornata per riflettere la piena esposizione del codice sorgente dell'applicazione attraverso mappe dei sorgenti accessibili al pubblico.

1. Leggi il riepilogo per capire come è stato modificato il risultato prima di decidere come agire in base ad esso.
2. Per sostituire un risultato personalizzato, modificalo nuovamente come faresti con qualsiasi altro risultato (ad esempio, modifica la gravità o il punteggio di rischio). La modifica più recente ha sempre la precedenza: AWS Security Agent impara da essa e applica la preferenza aggiornata alla prossima esecuzione, sostituendo la regola precedente.

> **Note**
>
> Le modifiche alla personalizzazione modificano gli attributi di ricerca come RiskLevel, RiskScore, nome, descrizione, ragionamento e AttackScript per riflettere gli standard che

AWS Security Agent ha appreso dalle tue modifiche. Qualsiasi campo che hai modificato in precedenza potrebbe essere modificato in base a risultati simili nelle esecuzioni future.

In che modo la personalizzazione impara dalle tue modifiche

Quando Findings Personalization è abilitato, AWS Security Agent apprende da tutte le modifiche apportate ai risultati e applica modifiche simili alle esecuzioni future. Qualsiasi campo modificato (come elencato nella precedente sezione Modifica risultati) verrà utilizzato per affinare le preferenze apprese dall'agente.

> **Note**
>
> Per il campo dello stato, solo la marcatura di un risultato come FALSE_POSITIVE viene considerata una preferenza apprendibile. Le modifiche ad altri valori di stato non innescano l'apprendimento.

Al prossimo pentest, l'agente valuta i nuovi risultati in base alle preferenze acquisite e applica le modifiche ove applicabili. Su ogni risultato modificato viene visualizzata una sezione sulle modifiche alla personalizzazione, che spiega le modifiche.

> **Note**
>
> La personalizzazione apprende solo dalle modifiche apportate nell'ultima esecuzione di pentest completata. La funzionalità deve essere abilitata al momento dell'inizio del pentest affinché avvenga l'apprendimento. Se modifichi lo stesso risultato in un'esecuzione successiva, la modifica più recente ha la precedenza: l'agente aggiorna le sue preferenze in base alla tua ultima decisione.

Abilita o disabilita la personalizzazione dei risultati

La personalizzazione dei risultati è abilitata per impostazione predefinita. Per disabilitarlo o riattivarlo:

1. Vai alla tua configurazione pentest.
2. Individua l'interruttore Findings Personalization.
3. Per abilitare la personalizzazione dei risultati, attiva l'interruttore. Per disattivarlo, disattivalo.

Se disabilitati, i risultati vengono visualizzati nello stato grezzo prodotto dall'agente senza alcuna personalizzazione applicata. Le preferenze apprese in precedenza vengono conservate e verranno nuovamente applicate se la funzionalità viene riattivata.

Fase 7: Interpretare le metriche CVSS

La comprensione delle metriche CVSS aiuta a valutare la vera gravità e a dare priorità agli interventi di correzione.

Quando esamini la sezione Ragionamento, presta attenzione a queste metriche chiave:

- Attack Vector (Network/Adjacent/Local/Physical): indica la distanza con cui l'attacco può essere eseguito
- Complessità dell'attacco (Low/High): mostra se sono necessarie condizioni speciali per lo sfruttamento
- Privilegi richiesti (None/Low/High): identifica il livello di accesso di cui ha bisogno un aggressore
- Interazione utente (None/Required): determina se l'exploit richiede il coinvolgimento dell'utente
- Confidentiality/Integrity/Availability Impact (None/Low/High): misura l'impatto sulla sicurezza del sistema

> **Important**
>
> I risultati ottenuti con Network Attack Vector, Bassa complessità e Alto confidentiality/integrity impatto rappresentano le vulnerabilità più pericolose che richiedono un'attenzione immediata.

Fase 8: Assegnare priorità e risolvere i risultati

Agisci in base ai risultati per correggere le vulnerabilità e migliorare il livello di sicurezza dell'applicazione.

Per risultati critici e di elevata gravità con elevata sicurezza:

1. Consulta la descrizione e i passaggi per riprodurre accuratamente le sezioni.
2. Accedi ai log dettagliati tramite il link «Trace actions & logs» per raccogliere prove complete.
3. Accedi a correzioni di codice pronte per l'implementazione tramite uno di questi metodi:
   - Per la riparazione automatica: utilizza il link pull request nella sezione sulla riparazione

- Per le richieste manuali: scegli «Codice di riparazione» nella pagina dei risultati per richiedere una pull request Prerequisiti:
- L'amministratore deve abilitare la correzione del codice per i GitHub repository nella console AWS Security Agent
- I repository devono essere inclusi nella configurazione pentest

4. Pianifica un test di penetrazione successivo per verificare che la correzione sia efficace.

Per i risultati di media e bassa gravità:

1. Assegna le priorità in base alla tua propensione al rischio e al contesto aziendale.
2. Includi le attività di correzione nella normale pianificazione dello sprint di sviluppo.
3. Valuta se più risultati di bassa gravità insieme creino un rischio maggiore.
4. Documenta tutti i rischi accettati con una giustificazione adeguata.

> **Important**
>
> Non ignorate i risultati di bassa gravità. Spesso è possibile unire più vulnerabilità a bassa gravità per creare exploit più gravi, specialmente se combinate con l'ingegneria sociale o l'accesso fisico.

Fase 9: Monitora l'avanzamento della riparazione

Utilizza l'interfaccia dei risultati per tracciare quali vulnerabilità sono state risolte e quali richiedono ulteriori azioni.

1. Mentre lavori alla correzione, consulta la sezione Passaggi per la riproduzione per verificare le correzioni.
2. Documenta il tuo approccio correttivo per ogni risultato per future verifiche di riferimento e di conformità.

> **Tip**
>
> Conserva un registro delle correzioni che associa ogni risultato alla relativa risoluzione, comprese le modifiche al codice, gli aggiornamenti della configurazione o le decisioni architettoniche prese per risolvere la vulnerabilità.

Fasi successive

Dopo aver esaminato i risultati del test di penetrazione:

- Assegna priorità ai risultati critici e di elevata gravità con la massima fiducia per una correzione immediata
- Scarica, rivedi ed esegui gli script di verifica nel tuo ambiente di test per testare gli script e identificare le vulnerabilità
- Crea ticket di tracciamento nel tuo sistema di gestione dei problemi con link per trovare dettagli e prove
- Implementa correzioni e controlli di sicurezza per risolvere le vulnerabilità identificate
- Monitora l'indicatore di avanzamento dell'esecuzione del test di penetrazione per individuare le vulnerabilità appena scoperte
- Pianifica un test di penetrazione successivo per verificare che le vulnerabilità siano state corrette correttamente
- Aggiorna il processo di test di sicurezza delle applicazioni e il modello di minaccia in base ai risultati
- Esamina le metriche CVSS per comprendere lo stato di sicurezza generale della tua applicazione

Per ulteriori informazioni sull'esecuzione dei test di penetrazione, consulta. the section called “Crea un test di penetrazione”

Per ulteriori informazioni sulla comprensione del ciclo di vita del Security Agent, vedere. the section called “Comprendi la gerarchia e il ciclo di vita delle risorse”

Fornisci credenziali di autenticazione per i test di penetrazione

Fornisci le credenziali per consentire ad AWS Security Agent di testare le aree autenticate delle tue applicazioni Web. Senza credenziali, l'agente può testare solo pagine e API accessibili al pubblico.

Configura le credenziali di autenticazione

1. Nel flusso di lavoro per la creazione del penetration test, individua la sezione Credenziali di autenticazione - Facoltativa.
2. Nella sezione Credential #1, scegli il metodo di immissione delle credenziali:
   - Inserisci credenziali: inserisci direttamente le credenziali. Ideale per ambienti di sviluppo e test.
   - Impostazione avanzata: utilizza la gestione AWS-native delle credenziali. Consigliato per ambienti di produzione e credenziali sensibili.

Opzioni avanzate

Se selezioni Impostazioni avanzate, puoi scegliere tra tre strategie di credenziali:

- Assunzione del ruolo IAM: per applicazioni che utilizzano AWS Cognito o l'autenticazione IAM
- AWS Secrets Manager: per lo storage sicuro delle credenziali con crittografia e rotazione
- Funzione Lambda: per la generazione dinamica di credenziali o flussi di autenticazione complessi

Inserisci direttamente le credenziali

1. Seleziona Inserisci credenziali.
2. Inserisci il nome utente e la password.
3. Nel menu a discesa URL di accesso, seleziona l'URL in cui verranno utilizzate queste credenziali. Deve essere selezionato dall'elenco degli endpoint di destinazione.
4. (Facoltativo) Nel campo 2FA - opzionale, fornisci un segreto TOTP per le applicazioni che richiedono l'autenticazione a due fattori. Puoi eseguire una delle seguenti operazioni:
   - Immettete direttamente il segreto TOTP (ad esempio,`JBSWY3DPEHPK3PXP`) o immettete l'`otpauth://totp/`URI completo (ad esempio,). `otpauth://totp/Example:user@example.com?secret=JBSWY3DPEHPK3PXP&issuer=Example`
   - Scegli l'icona di caricamento per caricare un'immagine del codice QR dalla pagina di configurazione dell'app di autenticazione. Il codice QR viene scansionato localmente e l'URI TOTP viene estratto automaticamente.

     Quando viene fornito un segreto TOTP, l'agente genera automaticamente nuovi codici monouso e li inserisce quando viene rilevato un prompt 2FA durante l'accesso.

5. (Facoltativo) Espandi la richiesta di accesso di Agent Space per fornire istruzioni di accesso specifiche se l'applicazione ha un flusso di autenticazione complesso.

> **Important**
>
> Utilizzate account di prova con accesso rappresentativo anziché account personali o amministrativi.

Usa impostazioni avanzate

Quando selezioni una strategia di credenziali avanzata (Secrets Manager, Lambda o ruolo IAM), AWS Security Agent recupera le credenziali direttamente dalla risorsa AWS configurata utilizzando il ruolo di servizio. Utilizza la richiesta di accesso di Agent Space per fornire all'agente istruzioni su come applicare tali credenziali all'applicazione, ad esempio, a quale URL di accesso accedere e quali campi del modulo compilare.

> **Note**
>
> I segreti di Secrets Manager e le funzioni Lambda devono trovarsi nello stesso account AWS della configurazione di AWS Security Agent. Cross-account le credenziali non sono attualmente supportate.

1. Seleziona Impostazioni avanzate.
2. Nel menu a discesa Strategia di accesso utente, scegli una delle seguenti opzioni:

Seleziona il ruolo IAM disponibile che l'agente deve assumere

Usa questa opzione per le applicazioni che utilizzano AWS Cognito, API Gateway con autenticazione IAM o altri sistemi di AWS-native autenticazione. Il ruolo IAM deve avere una relazione di fiducia che consenta ad AWS Security Agent di assumerlo e le autorizzazioni per accedere al sistema di autenticazione dell'applicazione.

Seleziona credenziali statiche da AWS Secrets Manager connesso

Usa questa opzione per recuperare le credenziali in modo sicuro da AWS Secrets Manager con crittografia, rotazione e controllo degli accessi.

Il ruolo IAM deve disporre di autorizzazioni e autorizzazioni. `secretsmanager:GetSecretValue` `secretsmanager:DescribeSecret`

L'agente recupera il valore segreto direttamente da Secrets Manager. Utilizzate la richiesta di accesso di Agent Space per indicare all'agente come applicare tali credenziali al flusso di accesso dell'applicazione, ad esempio, a quale URL accedere e quali campi del modulo compilare. Puoi utilizzare qualsiasi formato per memorizzare il tuo segreto, poiché l'agente interpreterà il formato utilizzando le istruzioni fornite nella richiesta di accesso.

Ad esempio, se l'agente deve inviare un modulo di username/password accesso all'indirizzohttps://example.com/login, puoi formattare il tuo segreto come JSON con i campi `username` and`password`. Se l'applicazione richiede l' TOTP-based autenticazione a due fattori, includi direttamente un `totpSecret` campo con il segreto TOTP o un URI completo: `otpauth://totp/`

```
{
  "username": "test-user",
  "password": "secure-password-here",
  "totpSecret": "JBSWY3DPEHPK3PXP"
}
```

Quindi, configura le istruzioni di autenticazione:. Imposta l'URL di accesso su `https://example.com` (o qualsiasi altro URL selezionato dall'elenco degli endpoint di destinazione). Inserisci quanto segue nella richiesta di accesso di Agent Space: «Vai al nome utente e la password forniti https://example.com/login e inserisci il nome utente e la password forniti nel modulo».

Come altro esempio, se invece hai una chiave API da fornire in un'intestazione HTTP, puoi memorizzarla come testo semplice:

```
"api-key-here"
```

Quindi, configura le istruzioni di autenticazione:. Inserisci quanto segue nella richiesta di accesso di Agent Space: «Imposta l' X-API-Key intestazione sulla chiave API fornita per tutte le richieste».

> **Important**
>
> È supportata solo la TOTP-based 2FA. SMS, e-mail, notifiche push, chiavi hardware e autenticazione OAuth non sono supportati.

Seleziona la funzione Lambda disponibile per recuperare le credenziali in modo dinamico

Utilizza questa opzione per sistemi di autenticazione complessi, generazione dinamica di credenziali o integrazione con provider di identità esterni.

Il ruolo IAM deve disporre di `lambda:InvokeFunction` autorizzazioni e la funzione deve essere completata entro 30 secondi.

Quando viene eseguito il penetration test, AWS Security Agent richiama la funzione AWS Lambda in modo sincrono e supera un evento che identifica il test di penetrazione e la credenziale specifica da risolvere:

```
{
  "pentest_arn": "arn:aws:securityagent:us-west-2:111122223333:pentest/pt-
abcd1234-5678-90ab-cdef-EXAMPLE11111",
  "actor_identifier": "Credential1"
}
```

- `pentest_arn`— L'Amazon Resource Name (ARN) del penetration test per il quale viene risolta la credenziale. Usalo per definire, autorizzare o controllare la richiesta all'interno della tua funzione.
- `actor_identifier`— Il nome della credenziale che hai assegnato a questa credenziale nella console (ad esempio,). `Credential1` Utilizzatelo per restituire la credenziale corretta quando una singola funzione serve più credenziali.

L'agente utilizza l'output della funzione direttamente come credenziale. Utilizza la richiesta di accesso di Agent Space per indicare all'agente come applicare tali credenziali alla tua applicazione, nello stesso modo in cui faresti con AWS Secrets Manager. the section called "Seleziona credenziali statiche da AWS Secrets Manager connesso"Per alcuni esempi su come formattare l'output della funzione Lambda e dei tipi di autenticazione supportati, consulta.

Configura più credenziali

Per testare diversi ruoli utente o sistemi di autenticazione:

1. Scegli Aggiungi un'altra credenziale.
2. Configura la credenziale aggiuntiva utilizzando uno dei due metodi di input.
3. Per rimuovere una credenziale, scegli Rimuovi nella sezione Credenziali.

Ottimizzazione degli accessi

L'ottimizzazione degli accessi consente ad AWS Security Agent di apprendere i modelli di navigazione delle precedenti esecuzioni di pentest e applicarli alle esecuzioni successive. Questi modelli includono flussi di accesso e flussi di lavoro di autenticazione in più fasi. Ciò riduce il tempo impiegato dall'agente per riscoprire le modalità di autenticazione, con conseguenti scansioni più rapide e una copertura dei test più coerente.

Come funziona l'ottimizzazione degli accessi

Alla prima esecuzione del pentest, l'agente scopre come navigare nel flusso di accesso dell'applicazione utilizzando le credenziali fornite dall'utente. Registra i passaggi di navigazione eseguiti con successo e genera un file di abilità che acquisisce il flusso di lavoro di accesso appreso.

Nelle esecuzioni successive, l'agente legge il file di abilità salvato e applica direttamente il modello di navigazione appreso, saltando la fase di scoperta. Ciò significa che:

- Tempi più rapidi per i test di autenticazione: l'agente applica immediatamente modelli di navigazione collaudati anziché esplorarli da zero
- Comportamento più coerente: l'agente segue lo stesso percorso collaudato anziché esplorare alternative

> **Note**
>
> Login Optimization apprende durante la prima sessione di accesso all'interno di una sessione. Le sessioni di accesso successive nella stessa sessione trarranno vantaggio da quanto appreso nella prima sessione. Nelle esecuzioni future, tutte le sessioni di accesso usufruiranno dell'abilità salvata.

Abilita o disabilita l'ottimizzazione degli accessi

L'ottimizzazione degli accessi è abilitata per impostazione predefinita. Per disabilitarlo o riattivarlo:

1. Nella configurazione pentest, vai alla sezione Credenziali di autenticazione - opzionale.
2. Individua l'interruttore di ottimizzazione del login.
3. Per abilitare l'ottimizzazione degli accessi, attiva l'interruttore. Per disabilitarlo, disattivalo.

Se disabilitato, l'agente rileva il flusso di accesso da zero a ogni esecuzione. Le abilità di navigazione acquisite in precedenza vengono mantenute e verranno nuovamente applicate se la funzionalità viene riattivata.

> **Tip**
>
> Se il flusso di accesso dell'applicazione cambia in modo significativo (ad esempio una pagina di accesso riprogettata o un nuovo passaggio di autenticazione), l'agente si adatta automaticamente aggiornando le competenze acquisite all'esecuzione successiva. Non è necessario reimpostare manualmente l'ottimizzazione.

Correggere un risultato del test di penetrazione

Quando visualizzi i risultati di un penetration test, puoi richiedere ad AWS Security Agent di tentare di correggere un risultato. Per i GitHub repository privati, AWS Security Agent apre una pull request con la correzione proposta. Per gli archivi pubblici, la correzione è disponibile come file diff scaricabile che puoi applicare localmente.

È necessario abilitare la ricerca di soluzioni correttive nella Console di gestione AWS. Consultare the section called "Consenti agli utenti di avviare la correzione dei risultati dei test di penetrazione e della revisione del codice". Gli utenti possono avviare la correzione di un risultato specifico dall'app Web AWS Security Agent.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Un test di penetrazione completato o in corso
- Accesso all'applicazione Web AWS Security Agent
- Familiarità con l'architettura e i requisiti di sicurezza dell'applicazione

Fase 1: abilitare o disabilitare la riparazione automatica

È possibile configurare le opzioni di correzione del codice quando si crea o si modifica un penetration test. Se abiliti la riparazione automatica, AWS Security Agent tenterà automaticamente di correggere i GitHub repository associati se l'agente conferma un risultato durante il pentest. Puoi anche avviare manualmente la correzione del codice. Nella visualizzazione per modificare i dettagli del test di

penetrazione, nella sezione Correzione automatica del codice, abilita o disabilita la correzione del codice.

Fase 2: Seleziona i repository per la correzione del codice

1. Scegli Avanti fino all'ultimo passaggio Risorse didattiche aggiuntive.
2. Scegli Seleziona tra le risorse.
3. Scegli i GitHub repository.
4. Seleziona i repository che desideri per la correzione del codice.
5. Salva il test di penetrazione.
6. Puoi vedere i repository associati con successo nella scheda Risorse didattiche per i test di penetrazione.

Fase 3: Avviare un test di penetrazione e visualizzare i risultati

Esegui il test di penetrazione per rilevare i risultati. Per ulteriori informazioni, consulta the section called “Esamina i risultati di un test di penetrazione”.

Fase 4: Avvia e visualizza la correzione del codice

1. Vai alla scoperta.
2. Se hai abilitato la correzione automatica del codice, verrà avviata una correzione del codice non appena AWS Security Agent avrà confermato un risultato.
3. Se desideri avviare manualmente una correzione del codice, scegli il pulsante Remediate code.
4. Nella sezione Code Remediation del risultato, puoi visualizzare lo stato della correzione del codice e i link alle pull request. Se il GitHub repository è pubblico, la correzione del codice è disponibile come file scaricabile anziché come richiesta pull. Puoi eseguire l'operazione `git apply /path/to/code_remediation_changes.diff` per applicare la modifica al tuo repository localmente.

Sicurezza e riferimento

Linee guida sulla sicurezza, quote di servizio e cronologia dei documenti per AWS Security Agent.

Sicurezza in AWS Security Agent

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue AWS Security Agent nel AWS cloud. Ciò include l'infrastruttura di servizio, i modelli di intelligenza artificiale e gli agenti di test di penetrazione. Third-party i revisori testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei programmi di AWS conformità.
- Sicurezza nel cloud - La tua responsabilità include le seguenti aree.
  - Gestione dell'accesso ad AWS Security Agent tramite policy e autorizzazioni IAM
  - Protezione dei contenuti forniti al servizio, inclusi documenti di progettazione, repository di codice e URL delle applicazioni per i test di penetrazione
  - Configurazione dei repository e delle applicazioni da monitorare
  - Esaminare e agire in base ai risultati di sicurezza forniti dal servizio
  - Protezione delle applicazioni in base alle linee guida fornite per la riparazione
  - La riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi AWS Security Agent.

Considerazioni sulla sicurezza per AWS Security Agent e test di penetrazione assistiti dall'intelligenza artificiale

AWS Security Agent è un agente di frontiera che protegge in modo proattivo le tue applicazioni durante tutto il ciclo di vita dello sviluppo in tutti i tuoi ambienti. Conduce revisioni di sicurezza automatizzate personalizzate in base alle tue esigenze, con i team di sicurezza che definiscono

centralmente gli standard che vengono convalidati automaticamente durante le revisioni. Security Agent esegue test di penetrazione su richiesta personalizzati in base all'applicazione, rilevando e segnalando rischi di sicurezza verificati. Questo approccio consente di scalare le competenze in materia di sicurezza tra le applicazioni per adeguarle alla velocità di sviluppo, fornendo al contempo una copertura di sicurezza completa. Integrando la sicurezza dalla progettazione all'implementazione, aiuta a prevenire le vulnerabilità in modo tempestivo e su larga scala.

I team di sicurezza definiscono i requisiti di sicurezza organizzativi una volta nella console AWS: librerie di autorizzazione approvate, standard di registrazione e politiche di accesso ai dati. AWS Security Agent applica automaticamente questi requisiti di sicurezza durante lo sviluppo, valutando i documenti e il codice dell'architettura rispetto agli standard e fornendo linee guida specifiche quando rileva violazioni. Ciò garantisce un'applicazione della sicurezza coerente tra i team e ridimensiona le revisioni in base alla velocità di sviluppo.

Per la convalida dell'implementazione, AWS Security Agent trasforma i test di penetrazione da collo di bottiglia periodico a funzionalità on-demand. I team di sicurezza forniscono gli URL di destinazione, i dettagli di autenticazione, il codice sorgente e la documentazione. AWS Security Agent sviluppa una comprensione approfondita delle applicazioni ed esegue sofisticate catene di attacco per scoprire e convalidare le vulnerabilità, consentendo ai team di eseguire test ogni volta che è necessario.

Funzionalità chiave

AWS Security Agent offre funzionalità di sicurezza complete che coprono l'intero ciclo di vita dello sviluppo.

Revisione della sicurezza del progetto

AWS Security Agent fornisce feedback sulla sicurezza su richiesta sui documenti di progettazione e valuta la conformità ai requisiti di sicurezza organizzativi prima della scrittura del codice. I team di sicurezza caricano i documenti di progettazione tramite l'applicazione Web, dove l'agente li analizza in base ai requisiti di sicurezza e presenta i risultati con linee guida per la correzione. In questo modo le revisioni manuali, che durano ore e ore, si trasformano in analisi mirate, permettendo ai team di risolvere i problemi di sicurezza nel momento in cui la correzione è più efficiente.

Revisione della sicurezza del codice

AWS Security Agent analizza le pull request o il codice caricato per verificare i requisiti di sicurezza organizzativi e i problemi di sicurezza più comuni, come la mancata convalida dell'input e i rischi di SQL injection. L'agente fornisce indicazioni per la correzione direttamente all'interno della tua

piattaforma di repository di codice. I team di sicurezza configurano i repository da monitorare, scalando la valutazione su tutte le basi di codice e mantenendo la supervisione sulle questioni critiche.

On-demand test di penetrazione

AWS Security Agent fornisce test di penetrazione su richiesta che rilevano e segnalano vulnerabilità di sicurezza convalidate attraverso scenari di attacco personalizzati in più fasi. AWS Security Agent distribuisce agenti di intelligenza artificiale specializzati che sviluppano il contesto applicativo sulla base della documentazione e delle credenziali fornite, quindi eseguono sofisticate catene di attacco per identificare vulnerabilità complesse che gli strumenti convenzionali non riescono a cogliere. Documenta i risultati con analisi d'impatto, percorsi di attacco riproducibili e correzioni di codice pronte per l'implementazione, accelerando i test di penetrazione da settimane a ore e scalando la convalida in tutto il portafoglio di applicazioni.

FAQs

Controllo di sicurezza &

In che modo AWS Security Agent autentica e mantiene l'accesso ai sistemi?

I test di penetrazione sono l'unica funzionalità di AWS Security Agent in grado di autenticarsi sul sistema di un utente in fase di esecuzione. L'AWS Security Agent accetta credenziali sotto forma di credenziali statiche di nome utente e password (archiviate in Secrets Manager) o un fornitore di credenziali (come funzione Lambda) come configurazione prima di iniziare il pen test. Queste credenziali vengono utilizzate per esercitare le normali funzionalità dell'utente durante il ciclo di vita del system/application pen test. Incoraggiamo gli utenti a creare nuove credenziali con autorizzazioni appropriate ai fini del pentesting.

Gli utenti possono controllare l'ambito e la profondità dei test per prevenire impatti indesiderati sul sistema?

AWS Security Agent consente ai clienti di selezionare una categoria specifica di vulnerabilità da esplorare in un endpoint. Gli utenti possono specificare URL non pertinenti per impedire ad AWS Security Agent di eseguire test di penetrazione su tali obiettivi. https://docs.aws.amazon.com/securityagent/latest/userguide/perform-penetration-test.html

Lo stesso AWS Security Agent può rappresentare un rischio per la sicurezza?

AWS Security Agent è incaricato di scoprire i rischi per la sicurezza, ma di farlo utilizzando intenzionalmente carichi d'impatto minimi (come estrarre la versione SQL invece di eliminare una

tabella quando viene scoperto un attacco di SQL injection). AWS Security Agent si limita inoltre a barriere deterministiche per prevenire comportamenti rischiosi come la creazione di un carico eccessivo sull'applicazione di destinazione. Sebbene esistano dei guardrail, potrebbero comunque verificarsi interazioni di logica aziendale involontarie o non ovvie, pertanto consigliamo sempre di eseguire test di penetrazione in un ambiente di preproduzione.

Quali dati raccoglie AWS Security Agent e dove vengono archiviati?

AWS Security Agent consente agli utenti di caricare artefatti per fornire un contesto sulla loro applicazione in fase di test. Per ulteriori informazioni sulla protezione dei dati, consulta. the section called "Protezione dei dati" AWS Security Agent selezionerà automaticamente la regione ottimale all'interno della tua area geografica per elaborare le tue richieste di inferenza. Ciò massimizza le risorse di elaborazione disponibili, la disponibilità dei modelli e offre la migliore esperienza del cliente. I dati rimarranno archiviati solo nella regione in cui ha avuto origine la richiesta, tuttavia, le richieste di input e i risultati di output potrebbero essere elaborati al di fuori di tale regione. Tutti i dati verranno trasmessi in modalità crittografata attraverso la rete sicura di Amazon. Per ulteriori informazioni, vedere Cross Region Inference.

Quali controlli sono presenti per bloccare i test non autorizzati su un endpoint?

Gli endpoint specificati come URL di destinazione per il pentesting richiederanno la convalida DNS o la convalida HTTP come misura della proprietà. AWS Security Agent chiederà al cliente di aggiungere un record TXT al DNS dell'endpoint o di esporre una route HTTP che restituisce una stringa di convalida come prova di proprietà. Solo dopo aver dimostrato la prova della proprietà, l'utente potrà procedere con un pentest. Le richieste a URL esterni agli URL di destinazione e accessibili verranno bloccate dalla rete.

I clienti hanno la responsabilità di assicurarsi di disporre dell'autorizzazione adeguata per testare tutti i sistemi che potrebbero essere interessati dalle loro attività di test di penetrazione. Tutti gli usi di AWS Security Agent devono essere conformi alla AWS Acceptable Use Policy (https://aws.amazon.com/aup/).

In che modo gli utenti bloccano e segnalano eventuali abusi utilizzando AWS Security Agent?

AWS Security Agent monitora continuamente le richieste e i tentativi di accesso a URL esterni agli URL di destinazione. Se viene rilevato un abuso, ad esempio il tentativo di utilizzare AWS Security Agent per condurre test non autorizzati su un endpoint di terze parti, tutti i pentest in corso nell'account verranno interrotti. I clienti possono contattare AWS Support o il team del proprio account AWS per ricevere assistenza.

AWS Security Agent può sostituire il flusso di lavoro di pen testing?

AWS Security Agent non è un servizio di penetration test professionale e incoraggiamo gli utenti a integrare AWS Security Agent nel loro flusso di lavoro di revisione della sicurezza. AWS Security Agent può fornire accessibilità ai test di penetrazione su richiesta durante la fase di sviluppo del ciclo di vita del software, quando coinvolgere professionisti del pentesting sarebbe troppo presto, poco pratico o avrebbe bisogno di essere rivalutato troppo frequentemente. I professionisti della sicurezza possono esaminare i risultati di AWS Security Agent per convalidarli, spiegarli o approfondirli per nuove scoperte (se esistenti).

Gli utenti possono configurare il controllo degli accessi basato sui ruoli (RBAC) per diversi membri del team?

Sì. AWS Security Agent si integra con AWS IAM Identity Center, consentendo agli amministratori di gestire i membri del team che possono accedere all'applicazione Web AWS Security Agent che consente agli utenti di creare, gestire e visualizzare revisioni di progettazione e pentest.

Funzionalità di test

Quali tipi di vulnerabilità può rilevare AWS Security Agent?

AWS Security Agent rileva le vulnerabilità nella Top 10 di OWASP per le applicazioni Web. AWS Security Agent fornisce tipi di rischio specifici che puoi includere o escludere nei test descritti di seguito. I risultati potrebbero derivare da queste categorie di rischio o da nuove scoperte scoperte seguendo le indicazioni di una combinazione di queste categorie di rischio.

- Caricamento arbitrario di file
  - Il caricamento arbitrario di file conferma che l'applicazione dovrebbe essere in grado di respingere file fasulli e dannosi in modo da proteggere l'applicazione e gli utenti
- Iniezione di codice
  - Code Injection è il termine generico per i tipi di attacco che consistono nell'iniettare codice che viene poi interpreted/executed immesso dall'applicazione
- Iniezione di comandi
  - L'iniezione di comandi è un attacco in cui l'obiettivo è l'esecuzione di comandi arbitrari sul sistema operativo host tramite un'applicazione vulnerabile
- Cross-Site Scripting (XSS)
  - Cross-Site Gli attacchi di scripting (XSS) sono un tipo di iniezione, in cui script dannosi vengono iniettati in siti Web altrimenti innocui e affidabili

- Riferimento diretto agli oggetti non sicuro
  - I riferimenti diretti agli oggetti (IDOR) insicuri si verificano quando un'applicazione fornisce l'accesso diretto agli oggetti in base all'input fornito dall'utente
- Vulnerabilità del token Web JSON
  - I JWT sono una fonte comune di vulnerabilità, sia nel modo in cui vengono implementati nelle applicazioni che nelle librerie sottostanti
- Inclusione di file locali
  - La vulnerabilità di inclusione dei file consente a un utente malintenzionato di includere un file, in genere sfruttando un meccanismo di «inclusione dinamica dei file» implementato nell'applicazione di destinazione
- Percorso di attraversamento
  - L'attacco Path Traversal (noto anche come directory traversal) mira ad accedere a file e directory archiviati all'esterno della cartella principale web
- Escalation dei privilegi
  - L'escalation dei privilegi si verifica quando un utente ottiene l'accesso a più risorse o funzionalità di quelle normalmente consentite e tale elevazione o modifica avrebbe dovuto essere impedita dall'applicazione
- Server-Side Request Forgery (SSRF)
  - Server-Side Request Forgery (SSRF) si verifica quando l'aggressore può sfruttare le funzionalità del server per leggere o aggiornare le risorse interne
- Server-Side Iniezione di modelli
  - Le vulnerabilità SSTI (Server Side Template Injection) si verificano quando l'input dell'utente viene incorporato in un modello in modo non sicuro e comporta l'esecuzione di codice in modalità remota sul server
- Iniezione SQL
  - L'attacco SQL injection consiste nell'inserimento o «iniezione» di una query SQL tramite i dati di input dal client all'applicazione
- Entità esterna XML
  - L'attacco XML External Entity è un tipo di attacco contro un'applicazione che analizza l'input XML. Questo attacco si verifica quando l'input XML contenente un riferimento a un'entità esterna viene elaborato da un parser XML configurato in modo debole

Quali metodi di autenticazione supporta AWS Security Agent?

AWS Security Agent supporta metodi di autenticazione comuni, tra cui OAuth e JWT. Per ulteriori informazioni, consulta la documentazione relativa ad .

In che modo AWS Security Agent gestisce la limitazione della velocità e la prevenzione del Denial of Service (DOS)?

AWS Security Agent dispone di barriere che impediscono l'interruzione o la disattivazione degli endpoint sottoposti a test, incluso il DOS. Dispone di controlli di velocità interni per rilevare e gestire modelli di traffico imprevisti.

AWS Security Agent può testare sia le API REST che GraphQL?

Sì, AWS Security Agent può testare gli endpoint delle API. Incoraggiamo i clienti a fornire la documentazione sulle API come risorse di apprendimento aggiuntive che consentono ad AWS Security Agent di avere un contesto migliore sulla forma e la funzionalità di ciascuna API testata.

In che modo gli utenti possono verificare che AWS Security Agent abbia coperto tutte le logiche e gli endpoint critici delle applicazioni?

AWS Security Agent effettuerà un'esplorazione approfondita delle applicazioni di destinazione e tenterà di esercitarla normalmente prima di tentare qualsiasi exploit. Ciò consente di acquisire una comprensione operativa dell'applicazione in fase di esecuzione e di scoprire la logica e gli endpoint critici dell'applicazione. Data la sua natura stocastica, non è garantito che AWS Security Agent scopra e testi tutte le applicazioni e gli endpoint critici per qualsiasi applicazione di destinazione. L'applicazione web AWS Security Agent offre visibilità su tutti gli endpoint scoperti e sulle azioni intraprese nei log dei test di penetrazione.

&Precisione e affidabilità

In che modo AWS Security Agent convalida i risultati prima della segnalazione?

AWS Security Agent utilizza validatori deterministici per aiutare a convalidare i risultati segnalati. Nei tipi di rischio in cui non è possibile utilizzare validatori deterministici, AWS Security Agent riprodurrà in modo indipendente le fasi di individuazione per acquisire fiducia nella validità del risultato. AWS Security Agent riporta solo i risultati ad alta o media confidenza e nasconde i risultati non verificati per impostazione predefinita.

AWS Security Agent può adattarsi alla logica applicativa personalizzata?

AWS Security Agent accetta facoltativamente codice sorgente, modello di minaccia, documenti di progettazione e documentazione API come risorse di apprendimento aggiuntive per ottenere un contesto diretto dall'utente sull'applicazione di destinazione utilizzata nel ciclo di vita di un pentest.

Gli utenti possono esaminare la metodologia di test di AWS Security Agent prima dell'esecuzione?

Al momento non è possibile visualizzare in anteprima la linea d'azione di AWS Security Agent. Il piano AWS Security Agent è di natura dinamica e si basa sull'esplorazione dell'applicazione di destinazione. I clienti possono monitorare AWS Security Agent durante l'esplorazione in tempo reale osservando i log dei test di penetrazione. Se i log mostrano una traiettoria non valida o indesiderata, i clienti possono interrompere l'esecuzione continua del pentest.

Installazione dell'integrazione &

AWS Security Agent si integra con strumenti di sicurezza (SIEM, gestione delle vulnerabilità) o CI/CD pipeline?

AWS Security Agent non si integra con strumenti o CI/CD pipeline di sicurezza esistenti.

In che modo AWS Security Agent gestisce le configurazioni specifiche dell'ambiente?

AWS Security Agent può essere configurato per essere eseguito con ruoli IAM specifici, all'interno di VPC, con credenziali pertinenti all'applicazione specificate dal cliente e con i repository di origine Github come riferimento del codice sorgente per l'applicazione di destinazione.

AWS Security Agent può funzionare in ambienti airgapped o isolati?

AWS Security Agent può essere configurato per avere connettività ai VPC, compresi quelli che non dispongono di accesso a Internet in uscita.

Più membri del team possono eseguire test contemporaneamente?

AWS Security Agent supporta 5 esecuzioni pentest simultanee per account, indipendentemente da chi avvia il test. I clienti possono creare un massimo di 100 Agent Spaces e 1.000 progetti Pentest.

Impatto operativo

Qual è l'impatto sulle prestazioni sui sistemi testati?

AWS Security Agent dispone di protezioni per impedire l'interruzione o la disattivazione degli endpoint sottoposti a test. Ciò include i controlli della velocità sul numero di chiamate che AWS Security Agent

può effettuare a un endpoint. Il sistema o l'endpoint in fase di test dovrebbero prevedere un aumento del traffico e l'attivazione di potenziali avvisi di monitoraggio a causa dell'attività di pen test. La nostra raccomandazione è di eseguire AWS Security Agent o qualsiasi attività di pen testing solo in ambienti di preproduzione.

Gli utenti possono pianificare o limitare AWS Security Agent?

AWS Security Agent non dispone di API pubbliche né della possibilità di pianificare le esecuzioni dei pen test. Inoltre, AWS Security Agent non offre un controllo simultaneo sulle richieste all'endpoint di destinazione all'avvio dell'esecuzione del pen test. Se AWS Security Agent causa problemi agli endpoint di destinazione, i clienti possono interrompere i pentest in corso.

Qual è la durata tipica di una valutazione completa della sicurezza?

Il tempo di esecuzione di ogni pentest dipende dall'ampiezza dell'applicazione di destinazione e dai tipi di rischio configurati per la valutazione. La maggior parte di pentest viene completata entro 16 ore.

Policy gestite da AWS per AWS Security Agents

Una policy gestita da AWS; è una policy standalone che viene creata e amministrata da AWS. Le policy gestite da AWS sono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy gestite da AWS potrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché sono disponibili per tutti i clienti AWS. Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle policy gestite da AWS. Se AWS aggiorna le autorizzazioni definite in una policy gestita da AWS, l'aggiornamento influisce su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la policy. È molto probabile che AWS aggiorni una policy gestita da AWS quando viene lanciato un nuovo servizio AWS o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consulta le policy gestite da AWS nella IAM User Guide.

Policy gestita da AWS: SecurityAgentWebAppAPIPolicy

Concede le autorizzazioni per interagire con l'API dell'applicazione Web Security Agent. Questa policy consente agli utenti di configurare ed eseguire test di penetrazione di sicurezza automatizzati, gestire le esecuzioni dei test, visualizzare i risultati di sicurezza e accedere alle risorse del Security

Agent. Questa policy fa riferimento al tipo di risorsa Agent Instance legacy e a specifiche azioni IAM legacy.

Dettagli delle autorizzazioni

Questa policy concede le autorizzazioni per interagire con il servizio Security Testing Control (securityagent: *) per:

- Pentest Management: crea, aggiorna, elimina ed elenca i penetration test e i relativi processi di esecuzione
- Risultati di sicurezza: Visualizza, descrivi e aggiorna i risultati di sicurezza dei test completati, inclusi i contenuti e i metadati correlati.
- Gestione delle attività: elenca e recupera le attività di revisione del codice e revisione della documentazione
- Resource Discovery: elenca e visualizza le istanze degli agenti, gli artefatti, le integrazioni e gli endpoint rilevati
- Esecuzione di test: avvia e interrompi le esecuzioni pentest con funzionalità di monitoraggio in tempo reale
- Correzione del codice: avvia la correzione automatica del codice per i problemi di sicurezza

Per visualizzare la versione più recente del documento sulla policy JSON, consulta SecurityAgentWebAppAPIPolicyla AWS Managed Policy Reference Guide.

Policy gestita da AWS: AWSSecurityAgentWebAppPolicy

Concede le autorizzazioni per interagire con l'API dell'applicazione Web Security Agent. Questa policy consente agli utenti di configurare ed eseguire test di penetrazione di sicurezza automatizzati, gestire le esecuzioni dei test, visualizzare i risultati di sicurezza e accedere alle risorse del Security Agent.

Dettagli delle autorizzazioni

Questa politica concede le autorizzazioni per interagire con il servizio Security Testing Control (securityagent: *) per:

- Pentest Management: crea, aggiorna, elimina ed elenca i penetration test e i relativi lavori
- Risultati di sicurezza: Visualizza, descrivi e aggiorna i risultati di sicurezza dei test completati, inclusi i contenuti e i metadati correlati.

- Gestione delle attività: elenca e recupera le attività di revisione del codice e revisione del progetto
- Resource Discovery: elenca e visualizza gli spazi degli agenti, gli artefatti, le integrazioni e gli endpoint rilevati
- Esecuzione dei test: avvia e interrompi i lavori pentest con funzionalità di monitoraggio in tempo reale
- Correzione del codice: avvia la correzione automatica del codice per i problemi di sicurezza

Per visualizzare la versione più recente del documento sulla policy JSON, consulta AWSSecurityAgentWebAppPolicyla AWS Managed Policy Reference Guide.

Aggiornamenti di AWS Security Agents alle policy gestite da AWS

Visualizza i dettagli sugli aggiornamenti delle policy gestite da AWS per AWS Security Agents da quando questo servizio ha iniziato a tracciare queste modifiche.

Per ricevere notifiche di tutte le modifiche al file di origine di questa pagina di documentazione specifica, puoi iscriverti al seguente URL con un lettore RSS:

Modifica	Descrizione	Data
Aggiunte autorizzazioni a AWSSecurityAgentWebAppPolicy.	Sono state aggiunte `TargetDomain` e autorizzazioni relative alle `DesignReviewFeedback` risorse per i nuovi tipi di risorse.	31 marzo 2026
È stata aggiunta una nuova politica AWSSecurityAgentWebAppPolicygestita.	È stata aggiunta una politica gestita `AWSSecurityAgentWebAppPolicy` per il nuovo tipo di AgentSpace risorsa e le modifiche al nome dell'azione IAM.	9 febbraio 2026
Aggiunte autorizzazioni a SecurityAgentWebApAPIPolicy.	Aggiunto `securityagent:StartCodeRemediation` per consentire agli utenti di avviare la correzion	20 gennaio 2026

Modifica	Descrizione	Data
	e automatica del codice per i problemi di sicurezza.	
Aggiunte autorizzazioni a SecurityAgentWebAppAPIPolicy.	`securityagent:BatchGetSecurityTestContentMetadata` Aggiunto per consentire agli utenti di visualizzare le immagini nella console.	5 dicembre 2025
Gli AWS Security Agents hanno iniziato a tracciare le modifiche.	AWS Security Agents ha iniziato a tracciare le modifiche per le sue policy gestite da AWS.	2 dicembre 2025

Protezione dei dati in AWS Security Agent

Il modello di responsabilità condivisa di AWS si applica alla protezione dei dati in AWS Security Agent. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che esegue tutto il cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Sei anche responsabile delle attività di configurazione e gestione della sicurezza per i servizi AWS che utilizzi. Per informazioni sulla protezione dei dati in Europa, consulta il post sul blog AWS Shared Responsibility Model e GDPR sull'AWS Security Blog. Per scopi di protezione dei dati, consigliamo di proteggere le credenziali dell'account AWS e configurare singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Usalo per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura API e registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail trail per acquisire le attività di AWS, consulta Working with CloudTrail trails nella AWS CloudTrail User Guide.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza predefiniti all'interno dei servizi AWS.

- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere ad AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con AWS Security Agent o altri servizi AWS utilizzando la console, l'API, l'AWS CLI o gli SDK AWS. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando si fornisce un URL a un server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Crittografia dei dati a riposo

AWS Security Agent crittografa tutti i dati inattivi utilizzando chiavi di AWS-managed crittografia per impostazione predefinita. Questo include:

- Documenti e codice di progettazione: tutti i documenti di progettazione, gli archivi di codice e gli artefatti applicativi forniti per le revisioni di sicurezza sono crittografati mediante crittografia. AES-256
- Risultati di sicurezza: tutti i risultati di sicurezza, i report sulle vulnerabilità e le raccomandazioni per la correzione sono crittografati quando sono inattivi.
- Dati di configurazione: i requisiti di sicurezza, le politiche personalizzate e le configurazioni dei servizi sono crittografati.
- Registri di controllo: tutti i registri delle attività di servizio e gli audit trail sono crittografati.

AWS Security Agent utilizza AWS Key Management Service (AWS KMS) per gestire le chiavi di crittografia. Facoltativamente, puoi utilizzare una chiave gestita dal cliente per crittografare i tuoi dati, ottenendo il pieno controllo sulle chiavi di crittografia che proteggono le tue risorse. Per ulteriori informazioni, consulta the section called "Chiavi gestite dal cliente".

Crittografia dei dati in transito

AWS Security Agent crittografa tutti i dati in transito utilizzando Transport Layer Security (TLS) 1.2 o versioni successive. Questo approccio si applica a:

- Comunicazioni API: tutte le chiamate API tra le tue applicazioni e AWS Security Agent utilizzano HTTPS con crittografia TLS.
- Accesso alla console: la console di AWS Security Agent è accessibile tramite HTTPS.
- Connessioni ai repository: le connessioni GitHub e altri repository di codice utilizzano protocolli crittografati.
- Comunicazioni con agenti: tutte le comunicazioni tra il servizio AWS Security Agent e gli agenti di penetration test utilizzano canali crittografati.

Gestione delle chiavi

AWS Security Agent utilizza AWS Key Management Service (AWS KMS) per gestire le chiavi di crittografia. Per impostazione predefinita, i dati vengono crittografati tramite AWS-managed chiavi. Facoltativamente, puoi specificare una chiave gestita dal cliente durante la creazione di risorse come Agent Spaces e integrazioni. Per ulteriori informazioni, consulta the section called “Chiavi gestite dal cliente”.

Riservatezza del traffico Internet

AWS Security Agent utilizza la rete Internet pubblica per comunicare con i provider di controllo del codice sorgente ospitati nel cloud (GitHub GitLab, Bitbucket) e Confluence Cloud.

Per i provider con hosting autonomo (GitLab Self-Managed GitHub Enterprise Server), puoi configurare connessioni private utilizzando Amazon VPC Lattice per mantenere tutto il traffico all'interno della rete AWS. Per ulteriori informazioni, consulta the section called “Connect al controllo del codice sorgente ospitato privatamente”.

Nella configurazione predefinita, AWS Security Agent utilizza la rete Internet pubblica per raggiungere l'app per i test di penetrazione. Facoltativamente, puoi configurare i test di penetrazione per utilizzare un VPC per accedere alla tua applicazione. Per ulteriori informazioni, consulta the section called “Connect agent a risorse VPC private”.

Cross-Region elaborazione dei dati

AWS Security Agent utilizza l'inferenza tra regioni per ottimizzare le risorse di calcolo disponibili e la disponibilità dei modelli. A seconda della regione in cui ha origine la richiesta, potremmo elaborare le richieste di input e i risultati di output in una regione diversa.

- Negli Stati Uniti orientali (Virginia settentrionale)`us-east-1`, Stati Uniti occidentali (Oregon)`us-west-2`, Asia Pacifico (Sydney)`ap-southeast-2`, Asia Pacifico (Tokyo)`ap-northeast-1`,

Europa (Francoforte) ed Europa (Irlanda)`eu-central-1`, `eu-west-1` AWS Security Agent utilizza l'inferenza geografica interregionale. Per la maggior parte delle funzionalità, l'elaborazione dei dati rimane entro i confini geografici (ad esempio Stati Uniti, UE, Australia o Giappone) da cui ha avuto origine la richiesta. Per quanto riguarda Code Remediation, le richieste provenienti da Australia e Giappone vengono elaborate nell'Unione Europea. Per i dettagli di routing specifici delle funzionalità, consulta la tabella Cross Region Inference.

- In Asia Pacifico (Mumbai)`ap-south-1`, Asia Pacifico (Singapore) e Sud America (San Paolo) `ap-southeast-1sa-east-1`, AWS Security Agent utilizza l'inferenza globale tra regioni. Potremmo elaborare richieste di input e risultati di output in qualsiasi regione AWS commerciale.

In tutti i casi, i dati rimangono archiviati solo nella regione in cui ha avuto origine la richiesta. Tutti i dati trasmessi durante le operazioni interregionali rimangono sulla rete AWS e non attraversano la rete Internet pubblica. Crittografiamo i dati in transito tra le regioni AWS.

Cross-Region l'inferenza è sempre abilitata e non può essere disattivata. Per informazioni dettagliate su quali regioni elaborano le richieste per ciascuna funzionalità, consulta la sezione Inferenza interregionale in. the section called “Best practice di sicurezza”

Eliminazione dei dati

Quando elimini dati da AWS Security Agent:

- I dati sono contrassegnati per l'eliminazione e non sono più accessibili tramite il servizio.
- I dati vengono eliminati da tutti i sistemi AWS Security Agent entro 30 giorni.

Per eliminare i tuoi dati

1. Nella console AWS, accedi ad AWS Security Agent.
2. Scegli i dati che desideri eliminare (revisioni di sicurezza, risultati o requisiti personalizzati).
3. Scegli Elimina e conferma l'eliminazione.

Gestione delle identità e degli accessi per AWS Security Agent

AWS Identity and Access Management (IAM) è un programma Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. IAM gli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle

autorizzazioni) a utilizzare le risorse di AWS Security Agent. IAM è un software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Destinatari

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

Utente del servizio: se utilizzi il servizio AWS Security Agent per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di AWS Security Agent per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso consente di richiedere le autorizzazioni corrette all'amministratore.

Se non riesci ad accedere a una funzionalità in AWS Security Agent, consultathe section called "Risoluzione dei problemi di identità e accesso ad AWS Security Agent".

Amministratore del servizio: se sei responsabile delle risorse di AWS Security Agent presso la tua azienda, probabilmente hai pieno accesso ad AWS Security Agent. È tuo compito determinare a quali funzionalità e risorse di AWS Security Agent devono accedere gli utenti del servizio. Devi quindi inviare richieste all' IAM amministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base di IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM AWS Security Agent, consultathe section called "Come funziona AWS Security Agent con IAM".

IAM amministratore - Se sei un IAM amministratore, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso ad AWS Security Agent. Per visualizzare esempi di policy basate sull'identità di AWS Security Agent che puoi utilizzare, consulta IAM. the section called "Esempi di policy basate sull'identità di AWS Security Agent"

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti (accedere a AWS) come utente root dell'account AWS o assumere un IAM ruolo. Utente IAM AWS suggerisce di utilizzare un ruolo IAM ed evitare di utilizzare direttamente l'utente root.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. Centro identità AWS IAM (IAM Identity Center) gli utenti, l'autenticazione Single Sign-On della tua azienda e le tue credenziali Google o Facebook sono esempi di identità federate. Quando

accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al Console di gestione AWS o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, consulta How to access to your AWS Account nella AWS Sign-In User Guide.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta il processo di firma Signature versione 4 nell'AWS General Reference.

Indipendentemente dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Multi-factor l'autenticazione nella Guida per l'utente di AWS IAM Identity Center (successore di AWS Single Sign-On) e l'utilizzo dell'autenticazione a più fattori (MFA) in AWS nella IAM User Guide.

Utente root dell'account AWS

La prima volta che crei un'identità Account AWS, inizi con un'identità a accesso singolo che ha accesso completo a tutte Servizi AWS le risorse dell'account. Tale identità è detta utente root dell'account AWS e puoi accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida di riferimento per la gestione degli account.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web Servizio di directory AWS, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare Centro identità AWS IAM. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center (successore di AWS Single Sign-On).

Utenti IAM e gruppi

An Utente IAMè un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare Utenti IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine Utenti IAM, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un IAM gruppo è un'identità che specifica un insieme di. Utenti IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni di set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo chiamato IamAdmins e concedere a quel gruppo le autorizzazioni per amministrare le risorse. IAM

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali permanenti a lungo termine, ma i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un Utente IAM (anziché un ruolo) nella Guida per l'utente IAM.

IAM roles

Un IAM ruolo è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a una persona Utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo in Console di gestione AWS cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, consulta Using IAM roles nella IAM User Guide.

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

- Accesso utente federato - Per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene

autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. Centro identità IAM mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare le risorse alle quali le identità possono accedere dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center (successore di AWS Single Sign-On).

- Utente IAM Autorizzazioni temporanee: An Utente IAM può assumere un IAM ruolo per acquisire temporaneamente autorizzazioni diverse per un'attività specifica.
- Cross-account accesso: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra i ruoli e le politiche basate sulle risorse per l'accesso tra account diversi, consulta How IAM roles differiscono dalle policy basate sulle risorse nella IAM User Guide.
- Cross-service accesso: alcuni utilizzano funzionalità in altri. Servizi AWS Servizi AWS Ad esempio, quando si effettua una chiamata in un servizio, è normale che tale servizio esegua applicazioni Amazon EC2 o in cui memorizzi oggetti Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, un ruolo di servizio oppure un ruolo collegato al servizio.
  - Autorizzazioni principali: quando utilizzi un ruolo Utente IAM o per eseguire azioni AWS, sei considerato un principale. Le policy concedono autorizzazioni a un'entità. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni.
  - Ruolo di servizio: un ruolo di servizio è un IAM ruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'interno IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Service-linked ruolo: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo di eseguire un'azione per conto dell'utente. Service-linked i ruoli vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.
- Applicazioni in esecuzione Amazon EC2 : è possibile utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un' Amazon EC2 istanza e che AWS

CLI effettuano richieste API. AWS Ciò è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' Amazon EC2 istanza. Per assegnare un AWS ruolo a un' Amazon EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' Amazon EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su Amazon EC2 istanze nella Guida per l'utente IAM.

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

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

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

Ogni IAM entità (utente o ruolo) inizia senza autorizzazioni. Di default, gli utenti non possono eseguire alcuna operazione, neppure modificare la propria password. Per autorizzare un utente a eseguire operazioni, un amministratore deve allegare una policy di autorizzazioni a tale utente. In alternativa, l'amministratore può aggiungere l'utente a un gruppo che dispone delle autorizzazioni desiderate. Quando un amministratore concede le autorizzazioni a un gruppo, a tutti gli utenti di quel gruppo vengono concesse tali autorizzazioni.

IAM le politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' Console di gestione AWS AWS CLI, dall'o dall' AWS API.

Identity-based politiche

Identity-based le politiche sono documenti relativi alle politiche di autorizzazione JSON che è possibile allegare a un'identità, ad esempio un Utente IAM ruolo o un gruppo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per scoprire come creare una policy basata sull'identità, consulta Creating IAM policies nella IAM User Guide.

Identity-based le politiche possono essere ulteriormente classificate come politiche in linea o politiche gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che è possibile allegare a più utenti, gruppi e ruoli all'interno del proprio. Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Resource-based politiche

Resource-based le politiche sono documenti di policy JSON allegati a una risorsa come un Amazon S3 bucket. Gli amministratori del servizio possono utilizzare queste politiche per definire quali azioni uno specifico principale (membro dell'account, utente o ruolo) può eseguire su quella risorsa e in quali condizioni. Resource-based le politiche sono politiche in linea. Non esistono policy basate su risorse gestite.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) sono un tipo di policy che stabilisce quali principali (membri, utenti o ruoli dell'account) dispongono delle autorizzazioni ad accedere a una risorsa. Gli ACL sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON. Amazon S3 AWS WAF, e Amazon VPC sono esempi di servizi che supportano gli ACL. Per maggiori informazioni sulle ACL, consulta la pagina Access Control List (ACL) overview nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai più tipi di policy comuni.

- Limiti delle autorizzazioni: un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (o ruolo). IAM Utente IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle politiche basate sull'identità dell'entità e dei relativi limiti di autorizzazione. Resource-based le politiche che specificano l'utente o il ruolo nel `Principal`

campo non sono limitate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le IAM entità nella Guida per l'utente IAM.

- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, è possibile applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account membri, compreso ogni utente root dell'account AWS. Per ulteriori informazioni su Organizations e SCP, consultare Come funzionano le SCP nella Guida per l'utente di AWS Organizations.
- Policy di sessione - Le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate sull'identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona AWS Security Agent con IAM

Prima di utilizzare IAM per gestire l'accesso ad AWS Security Agent, scopri quali IAM funzionalità sono disponibili per l'uso con AWS Security Agent.

Funzionalità IAM	Supporto per AWS Security Agent
the section called "Identity-based politiche per AWS Security Agent"	Sì
the section called "Resource-based politiche all'interno di AWS Security Agent"	No

Funzionalità IAM	Supporto per AWS Security Agent
the section called "Azioni politiche per AWS Security Agent"	Sì
the section called "Risorse relative alle policy per AWS Security Agent"	Parziale
the section called "Chiavi delle condizioni delle policy per AWS Security Agent"	Sì
the section called "Liste di controllo degli accessi (ACL) in AWS Security Agent"	No
the section called "Attribute-based controllo degli accessi (ABAC) con AWS Security Agent"	No
the section called "Utilizzo di credenziali temporanee con AWS Security Agent"	Sì
the section called "Sessioni di accesso diretto per AWS Security Agent"	Sì
the section called "Ruoli di servizio per AWS Security Agent"	No
the section called "Service-linked ruoli per AWS Security Agent"	Sì

Per avere una panoramica di alto livello su come Servizi AWS funzionano AWS Security Agent e altri IAM, consulta la sezione Servizi AWS Working with IAM nella IAM User Guide.

Identity-based politiche per AWS Security Agent

Supporta le policy basate sull'identità: sì

Identity-based le policy sono documenti di policy sulle autorizzazioni JSON che puoi allegare a un'identità, ad esempio un utente IAM, un gruppo di utenti o un ruolo. Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni

su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente di IAM.

Con le policy IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. Non è possibile specificare il principale in una politica basata sull'identità perché si applica all'utente o al ruolo a cui è associata. Per maggiori informazioni su tutti gli elementi utilizzati in una policy JSON, consulta il riferimento agli elementi della policy IAM JSON nella IAM User Guide.

Identity-based esempi di policy per AWS Security Agent

Per visualizzare esempi di policy basate sull'identità di AWS Security Agent, consulta. the section called "Esempi di policy basate sull'identità di AWS Security Agent"

Resource-based politiche all'interno di AWS Security Agent

Supporta le policy basate su risorse: no

Resource-based le policy sono documenti di policy JSON che alleghi a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o servizi AWS.

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. L'aggiunta di un'entità principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa si trovano in diversi account AWS, un amministratore IAM nell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate sull'identità. Per ulteriori informazioni, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Azioni politiche per AWS Security Agent

Supporta azioni Sì

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

L'`Action`elemento di una politica IAM basata sull'identità descrive l'azione o le azioni specifiche che saranno consentite o negate dalla politica. Le azioni politiche in genere hanno lo stesso nome dell'operazione API associata AWS . L'operazione viene utilizzata in una policy per concedere le autorizzazioni di eseguire l'operazione associata.

Le azioni politiche in AWS Security Agent utilizzano il seguente prefisso prima dell'azione:`securityagent:`. Ad esempio, per concedere a qualcuno l'autorizzazione a creare un ambiente con il funzionamento dell'`CreateEnvironment`API AWS Security Agent, includi l'`securityagent:CreateEnvironment`azione nella sua policy. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. AWS Security Agent definisce il proprio set di azioni che descrivono le attività che è possibile eseguire con questo servizio.

Per specificare più azioni in una sola istruzione, separa ciascuna di esse con una virgola come mostrato di seguito:

```
"Action": [
      "securityagent:action1",
      "securityagent:action2"
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `List`, includi la seguente azione:

```
"Action": "securityagent:List*"
```

Risorse relative alle policy per AWS Security Agent

Supporto risorse policy: Parziale

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

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

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

```
"Resource": "*"
```

Alcune azioni API di AWS Security Agent supportano più risorse. Ad esempio, è possibile fare riferimento a più ambienti quando si chiama l'azione `ListEnvironments` API. Per specificare più risorse in una singola istruzione, separa gli ARN con le virgole.

```
"Resource": [
      "EXAMPLE-RESOURCE-1",
      "EXAMPLE-RESOURCE-2"
```

Ad esempio, la risorsa di ambiente AWS Security Agent ha il seguente ARN:

```
arn:${Partition}:securityagent:${Region}:${Account}:environment/${EnvironmentId}
```

Per specificare gli ambienti `my-environment-1` e `my-environment-2` nella dichiarazione, utilizza i seguenti ARN di esempio:

```
"Resource": [
        "arn:aws:securityagent:us-east-1:123456789012:environment/my-environment-1",
        "arn:aws:securityagent:us-east-1:123456789012:environment/my-environment-2"
```

Per specificare tutti gli ambienti che appartengono a un account specifico, usa il carattere jolly (*):

```
"Resource": "arn:aws:securityagent:us-east-1:123456789012:environment/*"
```

Chiavi delle condizioni delle policy per AWS Security Agent

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

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

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

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'0Roperazione logica. Tutte le condizioni devono essere soddisfatte prima che vengano concesse le autorizzazioni della dichiarazione.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi concedere l' Utente IAM autorizzazione ad accedere a una risorsa solo se è contrassegnata con Utente IAM il suo nome. Per ulteriori informazioni, consulta gli elementi delle IAM policy: variabili e tag nella IAM User Guide.

AWS Security Agent definisce il proprio set di chiavi di condizione e supporta anche l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Liste di controllo degli accessi (ACL) in AWS Security Agent

Supporta le ACL: no

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

Attribute-based controllo degli accessi (ABAC) con AWS Security Agent

Supporta ABAC (tag nelle policy): No

Utilizzo di credenziali temporanee con AWS Security Agent

Supporta le credenziali temporanee: sì

Alcuni servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, tra cui quali servizi AWS funzionano con credenziali temporanee, consulta la sezione Servizi AWS che funzionano con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi alla Console di gestione AWS utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi ad AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando si accede alla console come utente e poi si cambia ruolo. Per maggiori informazioni sullo scambio dei ruoli, consulta Passaggio da un ruolo utente a un ruolo IAM (console) nella Guida per l'utente di IAM.

Puoi creare manualmente credenziali temporanee utilizzando l'AWS CLI o l'API AWS. Puoi quindi utilizzare tali credenziali temporanee per accedere ad AWS. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per maggiori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Sessioni di accesso diretto per AWS Security Agent

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

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

Ruoli di servizio per AWS Security Agent

Supporta i ruoli di servizio: no

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta Creare un ruolo per delegare le autorizzazioni a un servizio AWS nella IAM User Guide.

Service-linked ruoli per AWS Security Agent

Supporta i ruoli collegati ai servizi: Sì

Un ruolo collegato a un servizio è un tipo di ruolo di servizio collegato a un servizio AWS. Il servizio può assumere il ruolo di eseguire un'azione per tuo conto. Service-linked i ruoli vengono visualizzati nel tuo account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Esempi di policy basate sull'identità di AWS Security Agent

Per impostazione predefinita, Utenti IAM i ruoli non dispongono dell'autorizzazione per creare o modificare le risorse di AWS Security Agent. Inoltre, non possono eseguire attività utilizzando l'

AWS API Console di gestione AWS AWS CLI, o. Un IAM amministratore deve creare IAM politiche che concedano a utenti e ruoli l'autorizzazione a eseguire operazioni API specifiche sulle risorse specifiche di cui ha bisogno. L'amministratore deve quindi allegare tali politiche agli Utenti IAM o ai gruppi che richiedono tali autorizzazioni.

Per scoprire come creare una policy basata sull'identità IAM utilizzando questi esempi di documenti di policy JSON, consulta Creating policies using the JSON editor nella IAM User Guide.

Best practice per le policy

Identity-based le policy determinano se qualcuno può creare, accedere o eliminare le risorse di AWS Security Agent nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta le policy AWS gestite o le policy gestite di AWS per le funzioni lavorative nella IAM User Guide.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM policy, concedi solo le autorizzazioni necessarie per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per ulteriori informazioni sull'utilizzo IAM per applicare le autorizzazioni, consulta Policies and permissions nella IAM User Guide. IAM
- Utilizza le condizioni nelle IAM policy per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue policy per limitare l'accesso ad azioni e risorse. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. È inoltre possibile utilizzare le condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per ulteriori informazioni, consulta IAM JSON Policy elements: condition nella IAM User Guide.
- IAM Access Analyzer Utilizzalo per convalidare le IAM policy per garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy (JSON) e alle best practice. IAM IAM Access Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, consulta la convalida IAM Access Analyzer delle policy nella IAM User Guide.

- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che Utenti IAM richiede l'utilizzo di utenti root nel tuo account, attiva l'autenticazione a più fattori per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle MFA-protected API nella Guida per l'utente IAM.

Utilizzo della console AWS Security Agent

Per accedere alla console AWS Security Agent, un principale IAM deve disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentire al responsabile di elencare e visualizzare i dettagli sulle risorse di AWS Security Agent presenti nel tuo Account AWS. Se crei una policy di basata su identità più restrittiva delle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per i principali associati a tale policy.

Per garantire che i tuoi responsabili IAM possano ancora utilizzare la console AWS Security Agent, crea una policy con il tuo nome univoco. Allega la politica ai principali. Per ulteriori informazioni, consulta la sezione Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM:

Per i dettagli delle policy, consultathe section called “Policy gestita da AWS: SecurityAgentWebAppAPIPolicy”.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, è possibile accedere solo alle operazioni che soddisfano l'operazione API che stai cercando di eseguire.

Risoluzione dei problemi di identità e accesso ad AWS Security Agent

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere problemi comuni che potresti incontrare lavorando con AWS Security Agent e IAM.

AccessDeniedException

Se ricevi un'operazione API AWS `AccessDeniedException` quando chiami, le credenziali principali IAM che stai utilizzando non dispongono delle autorizzazioni necessarie per effettuare quella chiamata.

```
An error occurred (AccessDeniedException) when calling the CreateEnvironment operation:
User: arn:aws:iam::111122223333:user/user_name is not authorized to perform:
securityagent:CreateEnvironment on resource:
 arn:aws:securityagent:region:111122223333:environment/my-env
```

Nel messaggio di esempio precedente, l'utente non dispone delle autorizzazioni per chiamare l'operazione `CreateEnvironment` API di AWS Security Agent. Per fornire le autorizzazioni di amministratore di AWS Security Agent a un responsabile IAM, consultathe section called "Esempi di policy basate sull'identità di AWS Security Agent".

Per informazioni più generali su IAM, consulta Controllare l'accesso alle risorse AWS utilizzando le policy nella IAM User Guide.

Voglio consentire l'accesso a persone esterne al mio Account AWS per accedere alle mie risorse AWS Security Agent

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizzare tali policy per concedere alle persone l'accesso alle proprie risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Security Agent supporta queste funzionalità, consultathe section called "Come funziona AWS Security Agent con IAM".
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un Utente IAM altro Account AWS utente di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terzi nella Guida per l'utente IAM.
- Per capire come fornire l'accesso tramite la federazione delle identità, consulta Fornire accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per scoprire la differenza tra l'utilizzo dei ruoli e delle politiche basate sulle risorse per l'accesso tra account diversi, consulta How IAM roles differiscono dalle policy basate sulle risorse nella IAM User Guide.

Risposta agli incidenti

AWS Security Agent è un servizio proattivo di test di sicurezza progettato per identificare e prevenire le vulnerabilità prima che possano essere sfruttate. Il servizio si concentra sulla convalida preventiva della sicurezza attraverso revisioni di progettazione, analisi del codice e test di penetrazione piuttosto che sul rilevamento o sulla risposta reattivi agli incidenti.

Rilevamento degli incidenti

AWS Security Agent non fornisce funzionalità di rilevamento degli incidenti. Il servizio funziona come uno strumento proattivo di test di sicurezza che convalida le applicazioni per rilevare eventuali vulnerabilità durante lo sviluppo e prima della distribuzione. Per il monitoraggio della sicurezza in fase di esecuzione e il rilevamento degli incidenti, utilizza servizi come Amazon GuardDuty, AWS Security Hub o Amazon CloudWatch.

Avvisi sugli incidenti

AWS Security Agent non genera avvisi in tempo reale per incidenti di sicurezza. Il servizio fornisce risultati di sicurezza tramite la console AWS dopo aver completato revisioni di progettazione, analisi del codice o test di penetrazione. Questi risultati rappresentano potenziali vulnerabilità scoperte durante i test piuttosto che incidenti di sicurezza attivi.

Riparazione degli incidenti

AWS Security Agent non fornisce la risoluzione automatica degli incidenti. Il servizio identifica le vulnerabilità di sicurezza e fornisce linee guida per la correzione, tra cui:

- Descrizioni dettagliate delle vulnerabilità identificate
- Percorsi di exploit riproducibili per risultati convalidati
- Correzioni specifiche del codice e linee guida all'implementazione
- Analisi dell'impatto per i problemi rilevati

I team di sviluppo e sicurezza utilizzano queste linee guida per risolvere manualmente le vulnerabilità prima che raggiungano gli ambienti di produzione.

Supporto alle attività di risposta agli incidenti

Sebbene AWS Security Agent non sia progettato per la risposta agli incidenti, i team di sicurezza possono utilizzare il servizio per supportare le attività post-incidente:

Convalida delle vulnerabilità

Dopo un incidente di sicurezza, usa AWS Security Agent per verificare se esistono vulnerabilità simili in altre applicazioni o ambienti.

Valutazione del livello di sicurezza

Esegui test di penetrazione per convalidare i miglioramenti di sicurezza implementati come parte della risoluzione degli incidenti.

Analisi della causa principale

Utilizza le funzionalità di revisione della sicurezza del codice per identificare in che modo vulnerabilità simili potrebbero esistere in altre basi di codice.

Convalida della conformità per AWS Security Agent

Per sapere se un servizio AWS rientra nell'ambito di programmi di conformità specifici, consulta i servizi AWS in Scope by Compliance Program e scegli il programma di conformità che ti interessa. Per informazioni, consulta Programmi per la conformità di AWS.

Puoi scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Download dei rapporti in AWS Artifact.

La tua responsabilità di conformità quando utilizzi i servizi AWS è determinata dalla sensibilità dei tuoi dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS offre le risorse seguenti per facilitare la conformità:

- Governance e conformità per la sicurezza: queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- Riferimenti sui servizi conformi ai requisiti HIPAA - Elenca i servizi HIPAA idonei. Non tutti i servizi AWS sono idonei alla normativa HIPAA.
- Risorse per la conformità AWS - Questa raccolta di cartelle di lavoro e guide può essere utile al tuo settore e alla tua posizione.
- Guide alla conformità dei clienti AWS: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per proteggere i servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Council (PCI) e International Organization for Standardization (ISO)).
- Valutazione delle risorse con le regole nella Guida per gli sviluppatori di AWS Config: il servizio AWS Config valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti industriali.

- AWS Security Hub: questo servizio AWS offre una visione completa dello stato di sicurezza all'interno di AWS. Security Hub utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità rispetto agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: questo servizio AWS rileva potenziali minacce agli account, ai carichi di lavoro, ai contenitori e ai dati AWS monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager - Questo servizio AWS aiuta a controllare continuamente l'utilizzo del tuo AWS per semplificare la gestione dei rischi e la conformità alle normative e agli standard di settore.

Resilienza in AWS Security Agent

> **Note**
>
> AWS Security Agent è disponibile nelle seguenti regioni: Stati Uniti orientali (Virginia settentrionale) —`us-east-1`, Stati Uniti occidentali (Oregon) —`us-west-2`, Asia Pacifico (Mumbai) —`ap-south-1`, Asia Pacifico (Singapore) —`ap-southeast-1`, Asia Pacifico (Sydney) —`ap-southeast-2`, Asia Pacifico (Tokyo) —`ap-northeast-1`, Europa (Francoforte) —`eu-central-1`, Europa (Irlanda) — `eu-west-1` e Sud America (San Paolo) —. `sa-east-1` Utilizza l'inferenza tra regioni. In Asia Pacifico (Mumbai), Asia Pacifico (Singapore) e Sud America (San Paolo), AWS Security Agent utilizza l'inferenza globale tra regioni, che indirizza le richieste di inferenza verso qualsiasi regione AWS commerciale. In tutte le altre regioni, utilizza l'inferenza geografica interregionale, che mantiene l'elaborazione dei dati entro confini geografici specifici. AWS Security Agent è uno strumento utilizzato durante lo sviluppo di un'applicazione e non deve essere distribuito come infrastruttura critica o rivolta ai clienti.

L'infrastruttura globale di è basata su regioni e zone di disponibilità . Le regioni forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e velocità effettiva elevata. Con le zone di disponibilità è possibile progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza

interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle regioni e sulle zone di disponibilità AWS, consulta Infrastruttura globale di AWS.

Sicurezza dell'infrastruttura in AWS Security Agent

In quanto servizio gestito, AWS Security Agent è protetto dalla sicurezza di rete globale di AWS. Per informazioni sui servizi di sicurezza AWS e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo ambiente AWS utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, consulta Security in the AWS Well-Architected Framework.

Isolamento della rete

AWS Security Agent è un servizio completamente gestito accessibile tramite la console AWS e l'applicazione Web AWS Security Agent. L'accesso al servizio è controllato tramite AWS Identity and Access Management (IAM) o AWS IAM Identity Center, che possono integrarsi con il tuo provider di identità.

AWS Security Agent supporta gli endpoint VPC di interfaccia basati su AWS PrivateLink, consentendoti di accedere in modo privato alle API del servizio dal tuo VPC senza attraversare la rete Internet pubblica. Per ulteriori informazioni, consulta the section called "Endpoint VPC di interfaccia".

AWS Security Agent richiede l'accesso a Internet per eseguire test di penetrazione sulle applicazioni di destinazione e per le operazioni del piano di controllo. Il servizio utilizza l' AWS-managed infrastruttura per i test e non fornisce istanze EC2 o altre risorse di calcolo nel tuo account. Se configuri l'accesso VPC per i test di penetrazione, Security Agent crea un ENI nella sottorete, ma questo ENI non ha un indirizzo IP pubblico. Per ulteriori informazioni, consulta the section called "Connect agent a risorse VPC private".

Multi-tenancy e isolamento delle risorse

AWS Security Agent è un servizio multi-tenant. Le revisioni di sicurezza, i risultati e i dati dei clienti vengono isolati in singoli account AWS e crittografati su disco. AWS applica controlli standard di isolamento dell'infrastruttura per garantire che le attività di test di sicurezza di un cliente non influiscano sulle prestazioni o sulla riservatezza di un altro cliente.

AWS Security Agent e endpoint VPC di interfaccia (AWS PrivateLink)

Puoi usarlo AWS PrivateLink per creare una connessione privata tra il tuo VPC e AWS Security Agent. Puoi accedere a Security Agent come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione Direct Connect. Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per accedere a Security Agent.

Stabilisci questa connessione privata creando un endpoint di interfaccia attivato da AWS PrivateLink. In ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint di interfaccia. Si tratta di interfacce di rete gestite dai richiedenti che fungono da punto di ingresso per il traffico destinato a Security Agent.

Per ulteriori informazioni, consulta Accedere ai AWS servizi nella Guida AWS PrivateLink. AWS PrivateLink

Considerazioni per Security Agent

Prima di configurare un endpoint di interfaccia per Security Agent, consulta le considerazioni nella Guida. AWS PrivateLink

Security Agent supporta l'esecuzione di chiamate a tutte le sue azioni API dal tuo VPC, comprese le operazioni per la gestione degli spazi degli agenti, i test di penetrazione e i risultati di sicurezza.

È possibile selezionare IPv4, IPv6 o dualstack durante la creazione di un endpoint.

Le policy degli endpoint VPC sono supportate per Security Agent. Per impostazione predefinita, l'accesso completo a Security Agent è consentito tramite l'endpoint dell'interfaccia. È possibile controllare l'accesso allegando una policy dell'endpoint all'endpoint dell'interfaccia o associando un gruppo di sicurezza alle interfacce di rete dell'endpoint.

Tutte le chiamate API a Security Agent sono crittografate utilizzando TLS 1.2 o versioni successive, incluse le chiamate effettuate tramite endpoint VPC. Per ulteriori informazioni sulla protezione dei dati, consulta the section called “Protezione dei dati”. Le chiamate API di Security Agent vengono registrate. AWS CloudTrail Per ulteriori informazioni, consulta the section called “Esempio: voci dei file di registro di AWS Security Agent”.

Crea un endpoint di interfaccia per Security Agent

Puoi creare un endpoint di interfaccia per Security Agent utilizzando la console Amazon VPC o l'interfaccia a riga di comando (AWS AWS CLI). Per ulteriori informazioni, consulta Creare un endpoint di interfaccia nella Guida. AWS PrivateLink

Crea un endpoint di interfaccia per Security Agent utilizzando il seguente nome di servizio:

```
com.amazonaws.<region>.securityagent
```

Per creare l'endpoint dell'interfaccia utilizzando la AWS CLI, esegui il comando seguente. Sostituisci la regione, l'ID VPC, gli ID di sottorete e l'ID del gruppo di sicurezza con i tuoi valori.

```
aws ec2 create-vpc-endpoint \
    --vpc-id vpc-1a2b3c4d \
    --vpc-endpoint-type Interface \
    --service-name com.amazonaws.<region>.securityagent \
    --subnet-ids subnet-1a2b3c4d subnet-5e6f7a8b \
    --security-group-ids sg-1a2b3c4d \
    --private-dns-enabled
```

Important

Il DNS privato deve essere abilitato per l'endpoint dell'interfaccia. Security Agent richiede l'utilizzo del nome DNS regionale predefinito (ad esempio,`securityagent.us-east-1.api.aws`) per effettuare richieste API tramite l'endpoint. La chiamata diretta all'URL VPCE specifico dell'endpoint non è supportata.

Per utilizzare il DNS privato, devi impostare entrambi gli `enableDnsHostnames` attributi `enableDnsSupport` e `true` per il tuo VPC. Per ulteriori informazioni, consulta Attributi DNS per il VPC nella Guida per l'utente di Amazon VPC.

Configura i gruppi di sicurezza per l'endpoint dell'interfaccia

Quando si crea un endpoint di interfaccia, è possibile associare i gruppi di sicurezza alle interfacce di rete degli endpoint per controllare il traffico verso Security Agent. Crea un gruppo di sicurezza che consenta il traffico HTTPS in entrata (porta 443) dalle risorse del tuo VPC che devono comunicare con Security Agent.

Il gruppo di sicurezza deve includere la seguente regola in entrata:

- Tipo: HTTPS
- Protocollo: TCP
- Intervallo di porte: 443

- Fonte: il blocco CIDR VPC (ad esempio`10.0.0.0/16`) o gli ID dei gruppi di sicurezza delle risorse che richiedono l'accesso a Security Agent

Per ulteriori informazioni, consulta i gruppi di sicurezza nella AWS PrivateLink Guida.

Creazione di una policy dell' endpoint per l'endpoint dell'interfaccia

Una policy dell'endpoint è una risorsa IAM che è possibile allegare all'endpoint dell'interfaccia. La policy predefinita per gli endpoint consente l'accesso completo a Security Agent tramite l'endpoint dell'interfaccia. Per controllare l'accesso consentito a Security Agent dal tuo VPC, collega una policy endpoint personalizzata all'endpoint di interfaccia.

Una policy di endpoint specifica le informazioni riportate di seguito:

- I principali che possono eseguire azioni (AWS account, utenti IAM e ruoli IAM).
- Le azioni che possono essere eseguite.
- Le risorse in cui è possibile eseguire le operazioni.

Per ulteriori informazioni, consulta Controllare l'accesso ai servizi utilizzando le policy degli endpoint nella AWS PrivateLink Guida.

Esempio: policy degli endpoint VPC per AWS le azioni del Security Agent

Di seguito è riportato un esempio di policy sugli endpoint per AWS Security Agent. Se collegata a un endpoint, questa politica consente l'accesso alle azioni elencate del AWS Security Agent per tutti i principali su tutte le risorse.

```
{
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": [
            "securityagent:CreatePentest",
            "securityagent:ListPentests",
            "securityagent:BatchGetPentests",
            "securityagent:StartPentestExecution",
            "securityagent:StopPentestExecution",
            "securityagent:ListFindings",
```

```
            "securityagent:BatchGetFindings"
         ],
         "Resource": "*"
      }
   ]
}
```

Esempio: policy degli endpoint VPC che nega tutti gli accessi da un account specificato AWS

La seguente politica degli endpoint VPC nega all' AWS account `123456789012` tutti gli accessi alle risorse che utilizzano l'endpoint. La policy consente tutte le operazioni da altri account.

```
{
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": "securityagent:*",
         "Resource": "*"
      },
      {
         "Effect": "Deny",
         "Principal": {
            "AWS": "123456789012"
         },
         "Action": "securityagent:*",
         "Resource": "*"
      }
   ]
}
```

Risoluzione dei problemi

La connessione scade quando si chiama l'API di Security Agent

- Verifica che lo stato dell'endpoint VPC sia: `available`

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-1a2b3c4d \
    --query "VpcEndpoints[].State"
```

- Verifica che il gruppo di sicurezza associato all'endpoint consenta il traffico TCP in entrata sulla porta 443 dal tuo VPC CIDR o dal gruppo di sicurezza di origine.

- Verifica che le tabelle di routing VPC non indirizzino il traffico del Security Agent verso un gateway Internet o un gateway NAT anziché verso l'endpoint.

La risoluzione DNS non riesce per **`securityagent.<region>.api.aws`**

- Verifica che il DNS privato sia abilitato sull'endpoint:

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-1a2b3c4d \
    --query "VpcEndpoints[].PrivateDnsEnabled"
```

- Verifica che entrambi `enableDnsSupport` `enableDnsHostnames` siano impostati `true` sul tuo VPC:

```
aws ec2 describe-vpc-attribute --vpc-id vpc-1a2b3c4d --attribute enableDnsSupport
aws ec2 describe-vpc-attribute --vpc-id vpc-1a2b3c4d --attribute enableDnsHostnames
```

`Access denied`errori durante la chiamata delle API di Security Agent

- Controlla la policy degli endpoint VPC per assicurarti che consenta le azioni che stai tentando di eseguire.
- Verifica che la tua policy di identità IAM conceda le autorizzazioni richieste. `securityagent:`
- Se utilizzi una policy personalizzata per gli endpoint, conferma che sia la policy dell'endpoint che la policy IAM consentano la richiesta.

Analisi della configurazione e delle vulnerabilità in AWS Security Agent

Configurazione e controllo IT sono una responsabilità condivisa tra AWS e te, il nostro cliente. Per ulteriori informazioni, consulta il Modello di responsabilità condivisa AWS.

Cross-service confusa prevenzione sostitutiva

Con “confused deputy” si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. In AWS, l'impersonificazione tra servizi può dare origine al problema del vicesceriffo. Cross-service l'impersonificazione può verificarsi quando un servizio (il servizio chiamante) chiama un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui

normalmente non avrebbe accesso. Per evitare che ciò accada, AWS fornisce strumenti che ti aiutano a proteggere i tuoi dati per tutti i servizi con responsabili del servizio a cui è stato concesso l'accesso alle risorse del tuo account. Per ulteriori informazioni, consulta Cross-service Confused Deputy Prevention nella AWS Identity and Access Management User Guide.

Best practice di sicurezza per AWS Security Agent

AWS Security Agent offre una serie di funzionalità di sicurezza da prendere in considerazione durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, sono da considerare come considerazioni utili anziché prescrizioni.

Utilizza ambienti non di produzione per i test di penetrazione

AWS Security Agent utilizza una suite completa di strumenti di test di penetrazione della distribuzione Kali Linux. Questi strumenti sono progettati per identificare le vulnerabilità di sicurezza e possono eseguire azioni che modificano lo stato dell'applicazione, i dati o le configurazioni del sistema.

Procedura ottimale: esegui test di penetrazione su ambienti non di produzione che rispecchiano la configurazione di produzione. Questi ambienti di test dovrebbero:

- Non contenere dati reali dei clienti o informazioni di produzione sensibili
- Siate isolati dai sistemi di produzione
- Disponete di configurazioni e controlli di sicurezza simili a quelli di produzione
- Non utilizzare credenziali con accesso ai sistemi di produzione

I test in ambienti di produzione possono comportare:

- Modifica o cancellazione dei dati
- Interruzioni del servizio o peggioramento delle prestazioni
- Modifiche di stato non intenzionali
- Attivazione di avvisi di sicurezza o procedure di risposta agli incidenti

Convalida AI-generated i risultati di sicurezza

AWS Security Agent esegue analisi di sicurezza utilizzando agenti AI. A causa della natura non deterministica dei sistemi di intelligenza artificiale, i test di penetrazione possono produrre risultati diversi a seconda delle diverse esecuzioni.

Best practice: convalida i risultati di sicurezza prima di intraprendere azioni correttive:

- Esamina gli script di verifica generati da AWS Security Agent per ogni risultato
- Esegui script di verifica nel tuo ambiente di test per confermare la vulnerabilità
- Prendi in considerazione l'esecuzione di più test di penetrazione per garantire una copertura completa
- Applica un giudizio professionale in materia di sicurezza per valutare la gravità e la sfruttabilità dei risultati

Non tutti i problemi identificati possono rappresentare vulnerabilità sfruttabili nel contesto di implementazione specifico.

Rivedi e testa il codice di correzione generato

AWS Security Agent può generare correzioni di codice e miglioramenti della sicurezza per le vulnerabilità identificate. Queste AI-generated correzioni richiedono una verifica prima della distribuzione.

Procedura ottimale: esamina tutte le modifiche al codice generate:

- Esamina la completezza e la correttezza delle correzioni proposte
- Prova a fondo le correzioni in ambienti non di produzione
- Verifica che le correzioni non introducano nuove vulnerabilità o interrompano le funzionalità
- Usa AWS Security Agent per ripetere il test dopo aver applicato le correzioni o esegui gli script di verifica forniti
- Segui i processi di revisione e approvazione del codice della tua organizzazione

Accesso al repository di codice

AWS Security Agent può fornire indicazioni di sicurezza sulle modifiche al codice tramite commenti pull request e integrazione di revisione del codice. Per proteggere le informazioni di sicurezza sensibili, questa funzionalità opera in base a vincoli specifici.

Limitazione: le linee guida sulla sicurezza del codice sono limitate ai soli archivi privati. Ciò garantisce che:

- I risultati relativi alla sicurezza rimangono riservati per l'organizzazione
- Le potenziali vulnerabilità non vengono divulgate pubblicamente prima della correzione
- I consigli di correzione generati non rivelano i dettagli relativi allo sfruttamento

AWS Security Agent non fornisce linee guida sulla sicurezza del codice per gli archivi pubblici. Non rilascerà commenti su repository pubblici o progetti open source in cui i risultati di sicurezza sarebbero visibili pubblicamente.

I test di penetrazione di AWS Security Agent possono esaminare e correggere gli archivi privati e pubblici configurati per il pentest. Se il repository è pubblico, il codice di correzione verrà fornito come file diff scaricabile anziché come pull request.

URL accessibili

Gli URL accessibili specificano endpoint aggiuntivi a cui l'ambiente di test di penetrazione può accedere durante il test. Questi sono necessari quando l'applicazione dipende da servizi esterni come provider di autenticazione o CDN di terze parti. Tutte le dipendenze di rete richieste per il test devono essere specificate come URL di destinazione o URL accessibili. La rete blocca l'accesso a qualsiasi endpoint non specificato.

Implicazioni sulla sicurezza: AWS Security Agent non è incaricato di eseguire test di sicurezza su URL accessibili. Specificando gli URL accessibili, si indica la fiducia in queste dipendenze. I dati dei test di penetrazione, comprese le credenziali, possono essere trasmessi a questi endpoint URL accessibili durante il test.

Inferenza interregionale

AWS Security Agent seleziona automaticamente la regione ottimale per elaborare le richieste di inferenza. Ciò massimizza le risorse di elaborazione disponibili, la disponibilità dei modelli e offre la

migliore esperienza del cliente. I dati rimangono archiviati solo nella regione in cui ha avuto origine la richiesta; tuttavia, le richieste di input e i risultati di output potrebbero essere elaborati al di fuori di tale regione. Trasmettiamo tutti i dati crittografati attraverso la rete AWS.

AWS Security Agent utilizza due tipi di inferenza tra regioni a seconda della regione:

- Inferenza geografica interregionale: mantiene l'elaborazione dei dati entro confini geografici specifici (come Stati Uniti, UE, Australia o Giappone) per la maggior parte delle funzionalità. Per quanto riguarda Code Remediation, le richieste provenienti da Australia e Giappone vengono elaborate nell'Unione Europea. Utilizzato negli Stati Uniti orientali (Virginia settentrionale) —`us-east-1`, Stati Uniti occidentali (Oregon) —`us-west-2`, Asia Pacifico (Sydney) —`ap-southeast-2`, Asia Pacifico (Tokyo) —`ap-northeast-1`, Europa (Francoforte) — `eu-central-1` ed Europa (Irlanda) —. `eu-west-1`
- Inferenza globale tra regioni: indirizza le richieste di inferenza verso qualsiasi regione AWS commerciale, ottimizzando le risorse disponibili e garantendo un throughput del modello più elevato. Utilizzato in Asia Pacifico (Mumbai) —`ap-south-1`, Asia Pacifico (Singapore) — `ap-southeast-1` e Sud America (San Paolo) —`sa-east-1`.

Per le regioni che utilizzano l'inferenza globale tra regioni, i prompt di input e i risultati di output potrebbero essere elaborati in qualsiasi regione AWS commerciale. Tutti i dati trasmessi durante le operazioni interregionali rimangono sulla rete AWS e non attraversano la rete Internet pubblica. Crittografiamo i dati in transito tra le regioni AWS.

La tabella seguente descrive dove vengono elaborate le richieste di inferenza in base alla regione da cui proviene la richiesta e alla funzionalità utilizzata.

Origine della richiesta	Tutte le funzionalità tranne Code Remediation	Riparazione del codice
Stati Uniti — Stati Uniti orientali (Virginia settentrionale) `us-east-1` —, Stati Uniti occidentali (Oregon) — `us-west-2`	Stati Uniti	Stati Uniti
Unione europea — Europa (Irlanda) `eu-west-1` —,	Unione Europea	Unione Europea

Origine della richiesta	Tutte le funzionalità tranne Code Remediation	Riparazione del codice
Europa (Francoforte) — `eu-central-1`		
Australia — Asia Pacifico (Sydney) — `ap-southeast-2`	Australia	Unione Europea
Giappone — Asia Pacifico (Tokyo) — `ap-northeast-1`	Giappone	Unione Europea
Sud America — Sud America (San Paolo) — `sa-east-1`	Qualsiasi regione AWS commerciale	Qualsiasi regione AWS commerciale
India — Asia Pacifico (Mumbai) — `ap-south-1`	Qualsiasi regione AWS commerciale	Qualsiasi regione AWS commerciale
Sud-est asiatico - Asia Pacifico (Singapore) - `ap-southeast-1`	Qualsiasi regione AWS commerciale	Qualsiasi regione AWS commerciale

Cross-Region l'inferenza è sempre abilitata e non può essere disattivata. Cross-Region l'inferenza non è influenzata dalle politiche dei clienti nelle Service Control Policies (SCP) o AWS Control Tower che limitano i contenuti dei clienti a regioni specifiche. Per ulteriori informazioni su come AWS Security Agent protegge i dati durante l'elaborazione tra regioni, consulta elaborazione Cross-Region dei dati.

Azioni e migrazione delle risorse IAM

AWS Security Agent è un agente di frontiera che protegge in modo proattivo le tue applicazioni durante tutto il ciclo di vita dello sviluppo in tutti i tuoi ambienti. Se hai effettuato l'onboarding su AWS Security Agent prima del 9 febbraio 2026, sarai influenzato dalle modifiche imminenti il 9 marzo 2026 alle risorse esistenti di Agent Instance e alle azioni IAM di AWS Security Agent. In preparazione al rilascio del API/SDK supporto pubblico, la risorsa Agent Instance viene rinominata Agent Space e specifiche azioni IAM vengono rinominate. Queste modifiche influiranno su tutti i

ruoli IAM di Application o Agent Instances che hai creato prima del 9 marzo 2026. Per evitare di riscontrare problemi di autenticazione dopo il 9 marzo 2026, dovrai seguire la procedura descritta in Preparazione alla migrazione.

> **Note**
>
> Se crei nuove istanze di Agent dopo il 9 febbraio 2026, la nuova istanza dell'agente verrà creata come Agent Space e non sarà richiesta alcuna procedura di migrazione.

Modifiche pianificate

AWS Security Agent sta rinominando la risorsa Agent Instance in Agent Space: `arn:aws:securityagent:us-east-1:{{accountId}}:agent-instance/*` rinominata in. `arn:aws:securityagent:us-east-1:{{accountId}}:agent-space/*` Inoltre, le seguenti azioni IAM vengono rinominate:

- `securityagent:ListAgentInstances`rinominato in `securityagent:ListAgentSpaces`
- `securityagent:ListControls`rinominato in `securityagent:ListSecurityRequirements`
- `securityagent:BatchGetAgentInstances`rinominato in `securityagent:BatchGetAgentSpaces`
- `securityagent:BatchGetSecurityTestContentMetadata`rinominato in `securityagent:BatchGetPentestJobContentMetadata`
- `securityagent:BatchGetTasks`rinominato in `securityagent:BatchGetPentestJobTasks`
- `securityagent:CreateDocumentReview`rinominato in `securityagent:CreateDesignReview`
- `securityagent:GetDocumentReview`rinominato in `securityagent:GetDesignReview`
- `securityagent:GetDocumentReviewArtifact`rinominato in `securityagent:GetDesignReviewArtifact`
- `securityagent:ListDocumentReviews`rinominato in `securityagent:ListDesignReviews`
- `securityagent:ListDocumentReviewComments`rinominato in `securityagent:ListDesignReviewComments`
- `securityagent:ListTasks`rinominato in `securityagent:ListPentestJobTasks`

- `securityagent:StartPentestExecution`rinominato in `securityagent:StartPentestJob`
- `securityagent:StopPentestExecution`rinominato in `securityagent:StopPentestJob`
- `securityagent:DeleteDocumentReview`rinominato in `securityagent:DeleteDesignReview`

Preparazione alla migrazione

Per evitare di riscontrare problemi dopo il 9 marzo 2026 e continuare a utilizzare AWS Security Agent prima del 9 marzo 2026, dovrai affidarti alle nuove e vecchie risorse e alle azioni IAM nel tuo IAM roles/policies fino al 9 marzo 2026. Le istruzioni seguenti forniranno una guida per la migrazione ai nuovi formati di risorse e azioni:

1. Accedi al tuo account AWS e accedi alla console AWS Security Agent
2. Nel pannello di sinistra, seleziona Impostazioni e scegli il ruolo in Ruolo di servizio
3. Nella console IAM per il ruolo associato, seleziona Aggiungi autorizzazioni e Allega politiche
4. Seleziona AWSSecurityAgentWebAppPolicye scegli Aggiungi autorizzazioni
   a. Nota importante: verifica di aver selezionato AWSSecurityAgentWebAppPolicycome nuova politica e non SecurityAgentWebAppAPIPolicy
5. Verifica che il tuo ruolo IAM disponga ora di entrambe le politiche di autorizzazione AWSSecurityAgentWebAppPolicye che SecurityAgentWebAppAPIPolicyrientrino in questa categoria
6. Nella stessa console di ruolo IAM, seleziona Relazioni di fiducia, quindi Modifica politica di fiducia
7. Aggiorna la tua policy di fiducia nel seguente formato, sostituendo {{accountId}} con l'ID del tuo account AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "{{accountId}}"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:securityagent:us-east-1:{{accountId}}:application/*",
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-space/*",
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-instance/*"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:SetContext",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{accountId}}"
        },
        "ForAllValues:ArnEquals": {
          "sts:RequestContextProviders": "arn:aws:iam::aws:contextProvider/
IdentityCenter"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:securityagent:us-east-1:{{accountId}}:application/*",
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-space/*",
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-instance/*"
          ]
        }
      }
    }
  ]
}
```

8. Torna alla console di AWS Security Agent. Dal pannello di sinistra, seleziona Agent Spaces
9. Per ogni Agent Space di cui disponi con i test di penetrazione abilitati, esegui i seguenti passaggi
   a. Vai su Agent Space e seleziona Penetration test
   b. In Accesso al servizio, scegli il ruolo in Nome del ruolo di servizio

c. Nella console IAM per il ruolo associato, seleziona Relazioni di fiducia, quindi Modifica politica di fiducia

d. Aggiorna la tua policy di fiducia nel seguente formato, sostituendo {{accountId}} con l'ID del tuo account AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{accountId}}"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-space/*",
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-instance/*"
          ]
        }
      }
    }
  ]
}
```

Registrazione dei log AWS Chiamate API Security Agent con AWS CloudTrail

AWS Security Agent è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in AWS Security Agent. CloudTrail acquisisce tutte le chiamate API per AWS Security Agent come eventi. Le chiamate acquisite includono chiamate dalla console AWS di Security Agent e chiamate di codice alle operazioni dell'API AWS Security Agent. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per AWS Security Agent. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi.

Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a AWS Security Agent, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

AWS Informazioni su Security Agent in CloudTrail

CloudTrail è abilitato sull' AWS account al momento della creazione dell'account. Quando si verifica un'attività in AWS Security Agent, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per AWS Security Agent, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un percorso nella console, il percorso si applica a tutte le AWS regioni. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le azioni AWS di Security Agent vengono registrate da CloudTrail. Ad esempio, le chiamate a `CreatePentestBatchGetPentestJobs`, e `ListFindings` le azioni generano voci nei file di CloudTrail registro.

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

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).

- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Esempio: AWS Voci dei file di registro di Security Agent

Comprensione AWS Voci dei file di registro di Security Agent

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

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`CreatePentest`azione:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2025-01-15T10:30:00Z",
    "eventSource": "securityagent.amazonaws.com",
    "eventName": "CreatePentest",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.12",
    "userAgent": "aws-cli/2.13.0",
    "requestParameters": {
        "pentestName": "WebApp-Security-Test",
        "targetUrl": "https://example.com",
        "testScope": "OWASP-Top-10"
    },
    "responseElements": {
```

```
        "pentestId": "pt-1234567890abcdef0",
        "pentestArn": "arn:aws:securityagent:us-east-1:123456789012:pentest/
pt-1234567890abcdef0"
    },
    "requestID": "a1b2c3d4-e5f6-7890-abcd-ef1234567890",
    "eventID": "12345678-1234-1234-1234-123456789012",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Service Quotas

AWS Security Agent prevede quote che limitano il numero di risorse che puoi creare e la velocità con cui puoi eseguire le operazioni. Le quote contrassegnate come regolabili possono essere aumentate inviando una richiesta tramite AWS Support. Per ulteriori informazioni, consulta Creazione di casi di supporto e gestione dei casi.

Quote operative

Le quote operative limitano l'utilizzo mensile dei test di sicurezza e delle funzionalità di revisione per aiutare a gestire la capacità del servizio.

Risorsa	Scope	Quota	Regolabile
Revisioni dei progetti	Al mese per account per regione	200	Sì
Recensioni dei codici PR	Al mese per account per regione	1.000	Sì

Quote di configurazione

Le quote di configurazione limitano il numero di risorse e impostazioni che puoi configurare nel tuo ambiente AWS Security Agent.

Risorsa	Scope	Quota	Regolabile
Agent Spaces	Per account per regione	100	Sì
Integrazioni	Per account per regione	20	No
Risorse integrate per integrazione	Per integrazione	50	No
Requisiti di sicurezza personalizzati	Per account per regione	20	No
Progetti Pentest	Per account per regione	1.000	Sì
Esecuzioni simultanee di pentest	Per account per regione	5	Sì
Progetti di revisione del codice	Per account per regione	1.000	Sì
Esecuzioni simultanee di revisione del codice	Per account per regione	5	Sì

Cronologia dei documenti

La tabella seguente descrive alcuni dei principali aggiornamenti e nuove funzionalità della AWS Security Agents User Guide.

Modifica	Descrizione	Data
Connessioni private (anteprima)	Aggiunta documentazione per le connessioni private. Questa nuova funzionalità consente ad AWS Security Agent di connettersi ai sistemi di controllo del codice sorgente in esecuzione su reti private utilizzando Amazon VPC Lattice, senza esporre i sistemi alla rete Internet pubblica.	16 giugno 2026

Modellazione delle minacce (anteprima)	Documentazione aggiunta per la modellazione delle minacce. Questa nuova funzionalità crea un modello di minaccia dell'applicazione a partire da documenti di progettaz ione (documenti di ambito), codice sorgente (sorgenti) o entrambi. I documenti Scope sono documenti di progettazione delle funzional ità che definiscono l'obiettivo dell'analisi, mentre il codice sorgente fornisce un contesto sul sistema esistente. Se non fornisci i documenti relativi all'ambito, l'agente genera un modello di minaccia solo dal codice sorgente. Ogni esecuzione produce una panoramica del sistema e una serie di minacce classific ate per categoria STRIDE con valutazioni di gravità e raccomandazioni.	8 giugno 2026
Revisione completa del codice del repository (anteprima)	È stata aggiunta la documenta zione per la revisione completa del codice del repository. Questa nuova funzionalità esegue un'analis i di sicurezza sensibile al contesto dell'intero codebase e genera la correzione del codice per i risultati.	12 maggio 2026

Disponibilità regionale aggiornata per trovare soluzioni	La disponibilità delle regioni per i test di penetrazione, la ricerca di soluzioni nell'app Web AWS Security Agent è stata aggiornata.	16 aprile 2026
Disponibilità regionale aggiornata per consentire la ricerca di soluzioni	La disponibilità delle regioni per abilitare la correzione dei test di penetrazione mediante test di penetrazione nella Console di gestione AWS è stata aggiornata.	16 aprile 2026
Supporto delle chiavi gestite dal cliente	È stata aggiunta documenta zione per il supporto delle chiavi gestite dai clienti (CMK). Ora puoi specificare una chiave KMS gestita dal cliente durante la creazione di Agent Spaces e integrazioni per crittografare i dati con le chiavi che controlli tu.	31 marzo 2026
AWS aggiornamenti delle politiche gestiti	AWSSecurityAgentWe bAppPolicy È stata aggiunta una politica gestita per TargetDomain i nuovi tipi di DesignReviewFeedback risorse.	31 marzo 2026
AWS aggiornamenti delle politiche gestiti	AWSSecurityAgentWe bAppPolicy È stata aggiunta una politica gestita per il nuovo tipo di AgentSpace risorsa e le modifiche al nome dell'azione IAM.	9 febbraio 2026

AWS aggiornamenti delle politiche gestite	Aggiornato SecurityAgentWebAppAPIPolicy per consentire ai clienti di eliminare le recensioni dei progetti.	28 gennaio 2026
AWS aggiornamenti delle politiche gestiti	Aggiornato SecurityAgentWebAppAPIPolicy per consentire ai clienti di avviare la correzione automatica del codice per i problemi di sicurezza.	20 gennaio 2026
AWS aggiornamenti delle politiche gestite	Aggiornato SecurityAgentWebAppAPIPolicy per consentire ai clienti di visualizzare le immagini nella console.	5 dicembre 2025
Versione iniziale di AWS Security Agents	Documentazione iniziale per l'avvio del servizio	2 dicembre 2025

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.