Framework AWS Well-Architected

Pilastro della sicurezza

Pilastro della sicurezza: Framework AWS Well-Architected

Table of Contents

Pilastro della sicurezza - Framework AWS Well-Architected

Data di pubblicazione: 6 novembre 2024 (Revisioni del documento)

Il presente whitepaper tratta del pilastro della sicurezza del Framework AWS Well-Architected. Fornisce istruzioni per aiutarti ad applicare best practice e raccomandazioni correnti nella progettazione, distribuzione e manutenzione di carichi di lavoro sicuri in AWS.

Introduzione

Il Framework AWS Well-Architected aiuta a comprendere i pro e i contro delle decisioni che vengono prese durante la creazione di carichi di lavoro in AWS. Utilizzando il Framework, scoprirai le attuali best practice architetturali per progettare e gestire carichi di lavoro affidabili, sicuri, efficienti, convenienti e sostenibili nel cloud. Il Framework consente di misurare in modo coerente il carico di lavoro rispetto alle best practice e di identificare le aree da migliorare. Disporre di carichi di lavoro ben progettati aumenta notevolmente la probabilità di successo aziendale.

Il Framework si basa su sei pilastri:

- Eccellenza operativa
- Sicurezza
- Affidabilità
- Efficienza delle prestazioni
- Ottimizzazione dei costi
- Sostenibilità

Il presente documento tratta del pilastro della sicurezza. Ti aiuterà a soddisfare i requisiti aziendali e normativi seguendo le attuali raccomandazioni di AWS. È rivolto a coloro che ricoprono ruoli tecnologici, ad esempio direttori tecnici, responsabili della sicurezza delle informazioni, architetti, sviluppatori e membri dei team operativi.

Grazie a questo documento, comprenderai le attuali raccomandazioni e strategie di AWS da utilizzare durante la progettazione di architetture cloud incentrandole sulla sicurezza. Questo documento non fornisce dettagli sull'implementazione o modelli architetturali; tuttavia, include riferimenti alle risorse appropriate in cui trovare tali informazioni. Adottando le prassi di questo documento, puoi

creare architetture in grado di proteggere dati e sistemi, che controllino gli accessi e rispondano automaticamente agli eventi di sicurezza.

Nozioni di base sulla sicurezza

Il pilastro della sicurezza descrive come sfruttare le tecnologie cloud per proteggere dati, sistemi e risorse in modo da migliorare il livello di sicurezza. Il presente documento fornisce linee guida dettagliate sulle best practice per la progettazione di carichi di lavoro sicuri in AWS.

Principi di progettazione

Nel cloud sono presenti diversi principi utili per rafforzare la sicurezza del carico di lavoro:

- Implementazione di una solida base di identità: implementa il principio del privilegio minimo e applica la separazione dei compiti assegnando l'autorizzazione appropriata per ogni interazione con le risorse AWS. Centralizza la gestione delle identità e mira a eliminare la dipendenza dalle credenziali statiche a lungo termine.
- Mantenimento della tracciabilità: monitora, crea avvisi e verifica in tempo reale le operazioni e le modifiche apportate al tuo ambiente. Integra la raccolta di log e parametri con i sistemi per analizzare e intervenire automaticamente.
- Applicazione della sicurezza a tutti i livelli: applica un approccio di difesa avanzata con più controlli di sicurezza. Applicalo a tutti i livelli (ad esempio, edge di rete, VPC, bilanciamento del carico, ogni istanza e servizio di elaborazione, sistema operativo, applicazione e codice).
- Automatizzazione delle best practice di sicurezza: i meccanismi di sicurezza automatizzati basati su software migliorano la capacità di scalare le risorse in modo sicuro, più rapido e conveniente. Crea architetture sicure, compresa l'implementazione dei controlli, definite e gestite come codice nei modelli controllati dalle versioni.
- Protezione dei dati in transito e a riposo: classifica i dati in base a livelli di sensibilità e utilizza meccanismi quali crittografia, tokenizzazione e controllo degli accessi, ove opportuno.
- Accesso limitato delle persone ai dati: utilizza meccanismi e strumenti per ridurre o eliminare l'esigenza di accesso diretto o di elaborazione manuale dei dati. Ciò riduce il rischio di perdita, modifica e altri errori umani durante la gestione dei dati sensibili.
- Preparazione agli eventi di sicurezza: preparati per un incidente creando policy e processi di analisi e gestione degli incidenti in linea con i requisiti dell'organizzazione. Esegui simulazioni di risposta agli incidenti e utilizza strumenti dotati di automazione per aumentare la velocità nel rilevamento, nell'indagine e nel ripristino.

Definizione

La sicurezza nel cloud comprende sette aree:

- Nozioni di base sulla sicurezza
- Gestione dell'identità e degli accessi
- Rilevamento
- Protezione dell'infrastruttura
- Protezione dei dati
- Risposta agli incidenti
- Sicurezza delle applicazioni

Responsabilità condivisa

Sicurezza e conformità sono una responsabilità condivisa tra AWS e il cliente. Il modello condiviso può contribuire a ridurre l'onere operativo del cliente, dato che AWS rende operativi, gestisce e controlla tutti i componenti, dal sistema operativo host e il livello di virtualizzazione fino alla sicurezza fisica delle strutture in cui operano i servizi. Il cliente si assume la responsabilità della gestione del sistema operativo guest (con relativi aggiornamenti e patch di sicurezza), di altri software applicativi associati e della configurazione del firewall del gruppo di sicurezza fornito da AWS. I clienti devono valutare con attenzione i servizi scelti, dato che le loro responsabilità variano in base a servizi utilizzati, integrazione di tali servizi nel loro ambiente IT, leggi e regolamenti applicabili. La natura di questa responsabilità condivisa fornisce inoltre la flessibilità e il controllo dei clienti che consentono l'implementazione. Come mostrato nel grafico seguente, la distinzione della responsabilità è di solito riferita alla sicurezza "del" cloud rispetto alla sicurezza "nel" cloud.

La responsabilità di AWS per la "sicurezza del cloud": AWS è responsabile della protezione dell'infrastruttura su cui vengono eseguiti tutti i servizi offerti nell'AWS Cloud. L'infrastruttura è formata dai componenti hardware e software, dalle reti e dalle strutture che eseguono i servizi Cloud AWS.

La responsabilità del cliente per la "sicurezza nel cloud": la responsabilità del cliente sarà determinata dai servizi AWS Cloud che seleziona. Ciò determina la quantità di lavoro di configurazione che il cliente deve eseguire nell'ambito delle proprie responsabilità di sicurezza. Ad esempio, un servizio come Amazon Elastic Compute Cloud (Amazon EC2) è categorizzato come Infrastructure as a Service (IaaS) e, in quanto tale, richiede l'esecuzione da parte del cliente di tutte le attività inerenti la

gestione e la configurazione di sicurezza. I clienti che implementano un'istanza Amazon EC2 sono responsabili della gestione del sistema operativo guest (inclusi aggiornamenti e patch di sicurezza), di qualsiasi software applicativo o utilità installati dal cliente sulle istanze e della configurazione del firewall fornito da AWS (chiamato gruppo di sicurezza) su ciascuna istanza. Per i servizi astratti come Amazon S3 e Amazon DynamoDB, AWS si occupa del livello dell'infrastruttura, del sistema operativo e delle piattaforme, mentre i clienti accedono agli endpoint per archiviare e recuperare i dati. I clienti sono responsabili della gestione dei dati, incluse le opzioni di crittografia, della classificazione delle risorse e dell'utilizzo di strumenti IAM per applicare le autorizzazioni adeguate.

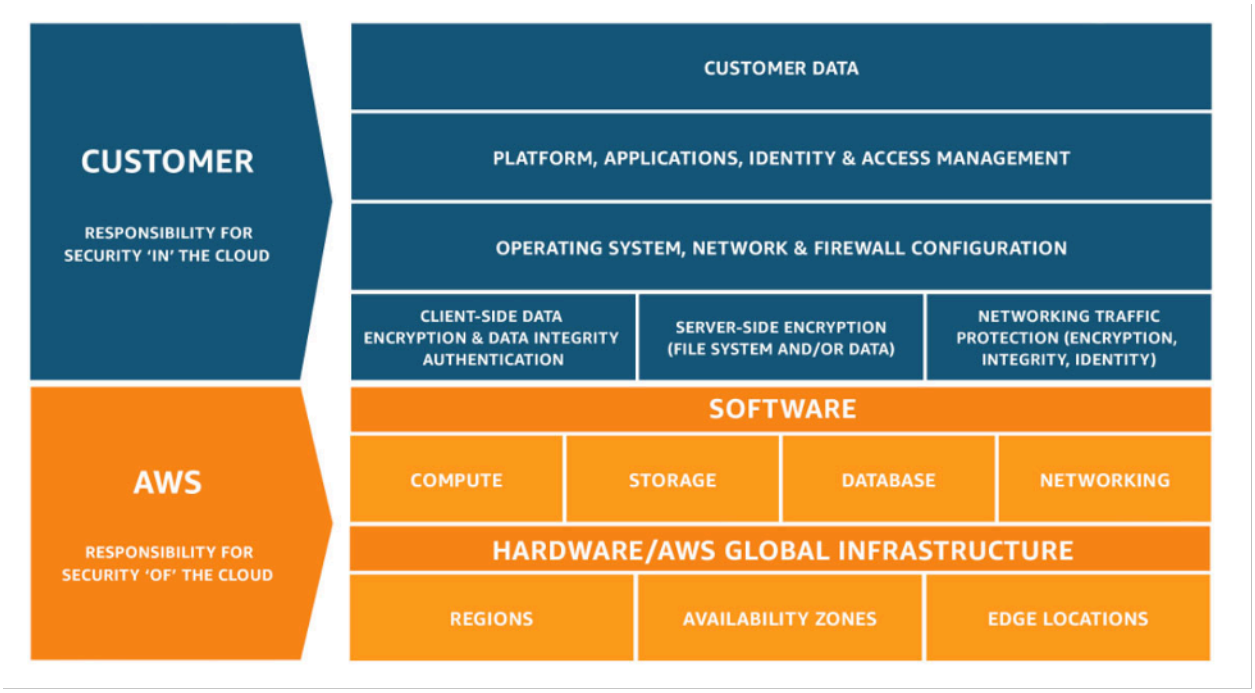


Figura 1: modello di responsabilità condivisa AWS.

Questo modello di responsabilità condivisa tra AWS/cliente si estende anche ai controlli IT. Così come la responsabilità di eseguire l'ambiente IT è condivisa tra AWS e i suoi clienti, allo stesso modo vengono condivisi gestione, operatività e verifica dei controlli IT. AWS può aiutare a sollevare il cliente dal peso di gestire i controlli, occupandosi di quelli associati all'infrastruttura fisica distribuita nell'ambiente AWS che in precedenza potevano essere gestiti dal cliente. Poiché ogni cliente in AWS presenta una diversa distribuzione, questi possono trarre vantaggio dal trasferimento della gestione di alcuni controlli IT ad AWS e ottenere un (nuovo) ambiente di controllo distribuito. I clienti possono quindi utilizzare la documentazione AWS su controllo e conformità a loro disposizione per eseguire le proprie procedure di valutazione e verifica dei controlli, come prescritto. I seguenti sono esempi di controlli gestiti da AWS, clienti AWS o entrambi.

Controlli ereditati: controlli che un cliente eredita completamente da AWS.

- Controlli fisici e ambientali

Controlli condivisi: controlli che si applicano sia a livello di infrastruttura sia a livello di cliente, ma in contesti o prospettive diversi. In un controllo condiviso, AWS offre i requisiti per l'infrastruttura e il cliente deve garantire l'implementazione dei controlli nell'ambito dell'utilizzo dei servizi AWS. Gli esempi includono:

- Gestione delle patch: AWS è responsabile dell'applicazione di patch e della risoluzione di difetti all'interno dell'infrastruttura, mentre i clienti sono responsabili dell'applicazione delle patch ai sistemi operativi e alle applicazioni guest.
- Gestione delle configurazioni:AWS mantiene la configurazione dei dispositivi dell'infrastruttura, mentre i clienti sono responsabili della configurazione di sistemi operativi, database e applicazioni guest.
- Consapevolezza e formazione: AWS forma i dipendenti AWS, mentre i clienti devono formare i propri dipendenti.

Specifici del cliente: controlli di cui sono responsabili esclusivamente i clienti in base all'applicazione implementata all'interno dei servizi AWS. Gli esempi includono:

- Protezione delle comunicazioni e dei servizi o sicurezza delle zone, che possono richiedere a un cliente di instradare o di suddividere in zone i dati all'interno di specifici ambienti di sicurezza.

Governance

La governance della sicurezza, come sottoinsieme dell'approccio generale, è mirata a supportare gli obiettivi aziendali definendo policy e controllando l'operato per contribuire alla gestione del rischio. Realizza la gestione del rischio seguendo un approccio a più livelli agli obiettivi di controllo di sicurezza, in cui ogni livello si sovrappone al precedente. Comprendere il modello di responsabilità condivisa AWS rappresenta il livello di partenza. Questa conoscenza offre una visione chiara delle responsabilità del cliente e di cosa viene ereditato da AWS. Una risorsa utile sono gli artefatti AWS, che consentono l'accesso on demand ai report di sicurezza e conformità di AWS e la selezione degli accordi online.

Soddisfa la maggior parte dei tuoi obiettivi di controllo del livello successivo. È qui che si trova la funzionalità della piattaforma. Ad esempio, questo livello include il processo di provisioning automatico dell'account AWS, l'integrazione con un gestore dell'identità digitale come AWS

IAM Identity Center e i controlli di rilevamento comuni. Qui si trovano anche alcuni degli output del processo di governance della piattaforma. Se vuoi iniziare a usare un nuovo servizio AWS, aggiorna le policy di controllo dei servizi (SCP) nel servizio AWS Organizations per fornire i guardrail per l'uso iniziale del servizio. Puoi usare altri SCP per implementare obiettivi di controllo della sicurezza comuni, a cui spesso ci si riferisce con il nome di invarianti di sicurezza. Si tratta di obiettivi o di configurazioni di controllo che applichi a più account, unità organizzative o all'intera organizzazione AWS. Esempi tipici sono: limitare le regioni di esecuzione dell'infrastruttura o prevenire la disattivazione dei controlli di rilevamento. Questo livello intermedio contiene anche policy codificate come regole di configurazione o verifiche nelle pipeline.

Il livello superiore è quello in cui i team di prodotto soddisfano gli obiettivi di controllo. Questo poiché l'implementazione avviene nelle applicazioni controllate dai team di prodotto. Potrebbe trattarsi dell'implementazione della convalida degli input in un'applicazione o della verifica del corretto passaggio dell'identità tra i microservizi. Anche se il team di prodotto possiede la configurazione, può ancora ereditare alcune funzionalità dal livello intermedio.

Ogni volta che implementi il controllo, l'obiettivo non cambia: gestire il rischio. Una gamma di framework di gestione del rischio si applica a regioni, settori o tecnologie specifici. Il tuo obiettivo principale: mettere in evidenza il rischio in base a probabilità e conseguenze. Questo è il rischio intrinseco. Puoi quindi definire un obiettivo di controllo che riduca la probabilità, le conseguenze o entrambi. Quindi, adottando un controllo, quale sarà probabilmente il rischio risultante. Questo è il rischio residuo. Gli obiettivi di controllo possono essere applicati a uno o più carichi di lavoro. Il diagramma seguente mostra una matrice di rischio tipica. La probabilità si basa sulla frequenza di casi precedenti, mentre le conseguenze si basano sui costi finanziari, reputazionali e in termini di tempo dell'evento.

Likelihood	Risk Level				
Very Likely	Low	Medium	High	Critical	Critical
Likely	Low	Medium	Medium	High	Critical
Possible	Low	Low	Medium	Medium	High
Unlikely	Low	Low	Medium	Medium	High
Very unlikely	Low	Low		Medium	High
Consequence	Minimal	Low	Medium	High	Severe

Figura 2: matrice della probabilità del livello di rischio

Gestione e separazione degli account AWS

Ti consigliamo di organizzare i carichi di lavoro in account e account di gruppo separati in base a funzione, requisiti di conformità o a un set comune di controlli anziché riflettere la struttura della creazione di report dell'organizzazione. In AWS, gli account rappresentano un confine rigido. Ad esempio, la separazione a livello di account è fortemente consigliata per isolare i carichi di lavoro di produzione dai carichi di lavoro di sviluppo e test.

Gestione centralizzata degli account: AWS Organizations automatizza la creazione e la gestione di account AWS e il relativo controllo dopo la loro creazione. Quando crei un account tramite AWS Organizations, è importante considerare l'indirizzo e-mail utilizzato, in quanto questo sarà l'utente root che consente la reimpostazione della password. Organizations consente di raggruppare gli account in unità organizzative (UO), che possono rappresentare ambienti diversi in base ai requisiti e allo scopo del carico di lavoro.

Impostazione dei controlli a livello centrale: controlla le operazioni che gli account AWS possono eseguire consentendo solo servizi, regioni e azioni del servizio specifici al livello appropriato. AWS Organizations consente di utilizzare le policy di controllo dei servizi (SCP) per applicare guardrail alle autorizzazioni a livello di organizzazione, unità organizzativa o account, validi per tutti gli i ruoli e utenti AWS Identity and Access Management (IAM). Ad esempio, è possibile applicare una SCP che limita agli utenti l'avvio di risorse in regioni che non sono state esplicitamente consentite. AWS Control Tower offre un modo semplificato per configurare e gestire più account. Automatizza la configurazione degli account in AWS Organizations, automatizza il provisioning, applica guardrail (che includono prevenzione e rilevamento) e fornisce un pannello di controllo per la visibilità.

Configurazione di servizi e risorse a livello centrale: AWS Organizations ti aiuta a configurare i servizi AWS applicabili a tutti i tuoi account. Ad esempio, puoi configurare la creazione di log centralizzata di tutte le operazioni eseguite nell'organizzazione utilizzando AWS CloudTrail, e impedire agli account membri di disabilitare tale funzione. Puoi inoltre aggregare a livello centrale i dati per le regole definite utilizzando AWS Config, in modo da eseguire l'audit dei tuoi carichi di lavoro per verificare la conformità e reagire rapidamente alle modifiche. AWS CloudFormation StackSets consente di gestire in modo centralizzato gli stack di AWS CloudFormation negli account e nelle unità organizzative della tua organizzazione. In questo modo puoi effettuare automaticamente il provisioning di un nuovo account per soddisfare i requisiti di sicurezza.

Usa la funzionalità di amministrazione delegata dei servizi di sicurezza per separare gli account utilizzati per la gestione dall'account (di gestione) della fatturazione dell'organizzazione. Diversi

servizi AWS, come GuardDuty, Security Hub e AWS Config, supportano le integrazioni con AWS Organizations, inclusa l'individuazione di un account specifico per le funzioni amministrative.

Best practice

- SEC01-BP01 Separazione dei carichi di lavoro tramite account
- SEC01-BP02 Utente root e proprietà dell'account sicuro

SEC01-BP01 Separazione dei carichi di lavoro tramite account

Definisci guardrail e isolamento comuni tra ambienti (ad esempio, quelli di produzione, sviluppo e test) e carichi di lavoro mediante una strategia multi-account. La separazione a livello di account è fortemente consigliata, in quanto fornisce un solido confine di isolamento in termini di sicurezza, fatturazione e accesso.

Risultato desiderato: una struttura di account in grado di isolare operazioni cloud, carichi di lavoro non correlati e ambienti in account separati, così da aumentare la sicurezza nell'infrastruttura cloud.

Anti-pattern comuni:

- Inserimento di più carichi di lavoro non correlati con diversi livelli di sensibilità dei dati nello stesso account.
- Scarsa definizione della struttura dell'unità organizzativa (UO).

Vantaggi dell'adozione di questa best practice:

- Riduzione dell'impatto in caso di accesso involontario a un carico di lavoro.
- Governance centralizzata dell'accesso a risorse, regioni e servizi AWS.
- Garanzia di sicurezza dell'infrastruttura cloud grazie a policy e amministrazione centralizzata dei servizi di sicurezza.
- Processo automatizzato di creazione e mantenimento dell'account.
- Audit centralizzati della tua infrastruttura per la conformità e i requisiti normativi.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Gli Account AWS offrono un confine di isolamento della sicurezza tra carichi di lavoro o risorse che operano a livelli di sensibilità diversi. AWS fornisce strumenti per gestire i carichi di lavoro del cloud su larga scala attraverso una strategia multi-account per sfruttare questo margine di isolamento. Per linee guida su concetti, modelli e implementazioni di strategie multi-account su AWS, consulta Organizing Your AWS Environment Using Multiple Accounts.

Se disponi di più Account AWS, organizza gli account in una gerarchia definita da livelli di unità organizzative (UO). I controlli di sicurezza possono quindi essere organizzati e applicati alle unità organizzative e agli account membri, stabilendo controlli preventivi coerenti sugli account membri dell'organizzazione. I controlli di sicurezza sono ereditati e consentono di filtrare le autorizzazioni disponibili per gli account membri situati ai livelli inferiori di una gerarchia di unità organizzative. Un buon progetto sfrutta questa ereditarietà per ridurre il numero e la complessità delle policy di sicurezza necessarie per raggiungere i controlli desiderati per ciascun account membro.

È possibile utilizzare due servizi, AWS Organizations e AWS Control Tower, per implementare e gestire questa struttura multi-account nel proprio ambiente AWS. AWS Organizations consente di organizzare gli account in una gerarchia definita da uno o più livelli di unità organizzative, con ciascuna di esse contenente un numero di account membri. Con le policy di controllo dei servizi, l'amministratore dell'organizzazione può stabilire controlli preventivi granulari sugli account membri, mentre AWS Config consente di definire controlli proattivi e investigativi sugli account membri. Molti servizi AWS si integrano con AWS Organizations per offrire controlli amministrativi delegati ed eseguire attività specifiche del servizio su tutti gli account membri dell'organizzazione.

Ripartito nei livelli di AWS Organizations, AWS Control Tower offre una configurazione immediata delle best practice per un ambiente AWS multi-account con una zona di destinazione. La zona di destinazione è il punto di ingresso nell'ambiente multi-account stabilito da Control Tower. Control Tower offre diversi vantaggi rispetto a AWS Organizations. Tre sono i vantaggi che consentono di migliorare la governance degli account:

- Controlli di sicurezza obbligatori integrati applicati in automatico agli account ammessi nell'organizzazione.
- Controlli opzionali attivabili o disattivabili per un determinato insieme di unità organizzative.
- AWS Control Tower Account Factory consente l'implementazione automatizzata di account contenenti linee di base e opzioni di configurazione preapprovate all'interno della tua organizzazione.

Passaggi dell'implementazione

1. Progettazione di una struttura delle unità organizzative: una struttura delle unità organizzative progettata in modo corretto riduce l'onere di gestione richiesto per creare e mantenere policy di controllo dei servizi e altri controlli di sicurezza. La struttura delle unità organizzative deve essere allineata a esigenze aziendali, sensibilità dei dati e struttura del carico di lavoro.
2. Creazione di una zona di destinazione per il tuo ambiente multi-account: una zona di destinazione costituisce una base infrastrutturale e di sicurezza coerente, che consente all'organizzazione di sviluppare, lanciare e implementare rapidamente carichi di lavoro. Puoi utilizzare una zona di destinazione AWS Control Tower personalizzata per orchestrare il tuo ambiente.
3. Definizione di guardrail: implementa guardrail di sicurezza coerenti per il tuo ambiente mediante la tua zona di destinazione. AWS Control Tower fornisce un elenco di controlli obbligatori e facoltativi implementabili. I controlli obbligatori vengono implementati in automatico in caso di utilizzo di Control Tower. Esamina l'elenco dei controlli altamente consigliati e facoltativi e adotta quelli più adatti alle tue esigenze.
4. Restrizione dell'accesso alle regioni aggiunte di recente: per le nuove Regioni AWS, le risorse IAM, ad esempio utenti e ruoli, verranno propagate solo alle regioni da te specificate. Puoi eseguire questa azione tramite la console in caso di utilizzo di Control Tower o modificando le policy di autorizzazione IAM in AWS Organizations.
5. Presa in esame di AWS CloudFormation StackSets: StackSets consente di implementare risorse, tra cui gruppi, ruoli e policy IAM in vari Account AWS e regioni a partire da un modello approvato.

Risorse

Best practice correlate:

- SEC02-BP04 Fai affidamento su un gestore dell'identità digitale centralizzato

Documenti correlati:

- AWS Control Tower
- Linee guida sugli audit di sicurezza AWS
- Best practice di IAM
- Use CloudFormation StackSets to provision resources across multiple Account AWS and regions
- Organizations FAQ

- AWS Organizations terminology and concepts
- Best Practices for Service Control Policies in an AWS Organizations Multi-Account Environment
- AWS Account Management Reference Guide
- Organizzazione dell'ambiente AWS che utilizza più account

Video correlati:

- Organizing Your AWS Environment Using Multiple Accounts
- Security Best Practices the Well-Architected Way
- Building and Governing Multiple Accounts using AWS Control Tower
- Abilitare Control Tower per le organizzazioni esistenti

SEC01-BP02 Utente root e proprietà dell'account sicuro

L'utente root è la figura più privilegiata di un Account AWS, ha pieno accesso amministrativo a tutte le risorse dell'account e, in alcuni casi, non può essere limitato dalle policy di sicurezza. Disattivare l'accesso programmatico all'utente root, stabilire controlli appropriati per l'utente root ed evitare l'uso di routine dell'utente root aiuta a ridurre il rischio di esposizione involontaria delle credenziali root e la conseguente compromissione dell'ambiente cloud.

Risultato desiderato: proteggere l'utente root riduce la possibilità di danni accidentali o intenzionali dovuti all'uso improprio delle credenziali dell'utente root. La creazione di controlli investigativi può anche permettere di avvisare il personale appropriato quando vengono eseguite azioni utilizzando l'utente root.

Anti-pattern comuni:

- Utilizzo dell'utente root per attività diverse da quelle che richiedono le proprie credenziali.
- Nessun test dei piani di emergenza su base regolare per verificare il funzionamento di infrastrutture critiche, processi e personale durante un'emergenza.
- Analisi limitata al tipico flusso di accesso all'account, trascurando di considerare o testare metodi alternativi di ripristino dell'account.
- Nessuna gestione di DNS, server di posta elettronica e provider telefonici come parte del perimetro di sicurezza critico, in quanto utilizzati nel flusso di recupero degli account.

Vantaggi dell'adozione di questa best practice: proteggere l'accesso all'utente root aumenta la sicurezza circa controlli e audit delle azioni nell'account

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

AWS offre molti strumenti per proteggere gli account. Tuttavia, poiché alcune di queste misure non sono attivate per impostazione predefinita, è necessario intervenire direttamente per implementarle. Queste raccomandazioni costituiscono i passi fondamentali per mettere in sicurezza il proprio Account AWS. Durante l'implementazione di questi passaggi, è importante creare un processo di valutazione e monitoraggio continuo dei controlli di sicurezza.

La prima creazione di un Account AWS parte con una singola identità che ha accesso completo a tutti i servizi e risorse AWS presenti nell'account. Questa identità è chiamata utente root dell'Account AWS. Puoi accedere come utente root utilizzando l'indirizzo e-mail e la password usati per creare l'account. A causa dell'accesso elevato concesso all'utente root AWS, è necessario limitare l'uso dell'utente root AWS all'esecuzione di attività che lo richiedano nello specifico. Le credenziali di accesso dell'utente root devono essere tenute sotto stretta sorveglianza e l'autenticazione a più fattori (MFA) deve essere sempre utilizzata per l'utente root dell'Account AWS.

Oltre al normale flusso di autenticazione per accedere all'utente root utilizzando un nome utente, una password e un dispositivo di autenticazione a più fattori (MFA), esistono flussi di recupero dell'account che consentono di accedere all'utente root dell'Account AWS grazie all'accesso all'indirizzo e-mail e al numero di telefono associati all'account. Pertanto, è altrettanto importante proteggere l'account e-mail dell'utente root a cui vengono inviati l'e-mail di recupero e il numero di telefono associato all'account. Prendi anche in considerazione le potenziali dipendenze circolari, quando l'indirizzo e-mail associato all'utente root è ospitato su server di posta elettronica o su risorse del servizio dei nomi di dominio (DNS) dello stesso Account AWS.

Quando si utilizza AWS Organizations, esistono più Account AWS, ciascuno con un utente root. Un account è designato come account di gestione e sotto l'account di gestione è possibile aggiungere diversi livelli di account membri. La priorità è proteggere l'utente root dell'account di gestione, quindi occuparsi degli utenti root degli account membri. La strategia per la protezione dell'utente root dell'account di gestione può essere diversa da quella degli utenti root degli account membri ed è possibile effettuare controlli di sicurezza preventivi sugli utenti root degli account membri.

Passaggi dell'implementazione

Per stabilire i controlli per l'utente root, si consigliano i seguenti passaggi di implementazione. Ove applicabile, le raccomandazioni devono essere confrontate con la versione 1.4.0 del benchmark CIS AWS Foundations. Oltre a questi passaggi, consulta le linee guida sulle best practice AWS per proteggere il tuo account Account AWS e le tue risorse.

Controlli preventivi

1. Imposta informazioni di contatto precise per l'account.
    a. Queste informazioni vengono utilizzate per il flusso di recupero della password persa, per il flusso di recupero dell'account del dispositivo MFA perso e per le comunicazioni critiche relative alla sicurezza con il team.
    b. Utilizza un indirizzo e-mail ospitato dal dominio aziendale, preferibilmente una lista di distribuzione, come indirizzo e-mail dell'utente root. L'utilizzo di una lista di distribuzione anziché l'account e-mail di un singolo individuo offre una maggiore ridondanza e continuità di accesso all'account root per lunghi periodi di tempo.
    c. Il numero di telefono indicato nelle informazioni di contatto deve essere dedicato e sicuro per questo scopo. Il numero di telefono non deve essere indicato o condiviso con nessuno.
2. Non creare chiavi di accesso per l'utente root. Se sono presenti chiavi di accesso, rimuovile (CIS 1.4).
    a. Elimina le credenziali programmatiche a lunga durata (chiavi di accesso e segrete) per l'utente root.
    b. Se esistono già chiavi di accesso dell'utente root, fai in modo che i processi che utilizzano tali chiavi passino all'utilizzo di chiavi di accesso temporanee provenienti da un ruolo AWS Identity and Access Management (IAM), quindi elimina le chiavi di accesso dell'utente root.
3. Stabilisci se è necessario memorizzare le credenziali per l'utente root.
    a. Se utilizzi AWS Organizations per creare nuovi account membri, la password iniziale dell'utente root sui nuovi account membro è impostata su un valore casuale che non è visibile a te. Prendi in considerazione l'utilizzo del flusso di reimpostazione della password del tuo account di gestione AWS Organization per accedere all'account membro, se necessario.
    b. Per gli Account AWS standalone o per l'account di gestione di AWS Organization, considera la creazione e l'archiviazione sicura delle credenziali per l'utente root. Usa MFA per l'utente root.
4. Usa i controlli preventivi per gli utenti root degli account membri in ambienti AWS multi-account.
    a. Prendi in considerazione l'utilizzo del guardrail preventivo Disallow Creation of Root Access Keys for Root User per gli account membri.

b. Prendi in considerazione l'utilizzo del guardrail preventivo Disallow Actions as a Root User per gli account membri.

5. Se sono necessarie le credenziali per l'utente root:
   a. Utilizza una password complessa.
   b. Attiva l'autenticazione a più fattori (MFA) per l'utente root, in particolare per gli account dei manager (paganti) AWS Organizations (CIS 1.5).
   c. Prendi in considerazione i dispositivi MFA hardware per la resilienza e la sicurezza, in quanto i dispositivi monouso possono ridurre le possibilità che i dispositivi contenenti i codici MFA vengano riutilizzati per altri scopi. Verifica che i dispositivi hardware MFA alimentati da una batteria siano sostituiti regolarmente. (CIS 1.6)
      - Per configurare l'MFA per l'utente root, segui le istruzioni per creare un dispositivo MFA virtuale o un dispositivo MFA hardware.
   d. Prendi in considerazione la registrazione di più dispositivi MFA per il backup. Sono consentiti fino a 8 dispositivi MFA per account.
      - Tieni presente che la registrazione di più di un dispositivo MFA per l'utente root disattiva in automatico il flusso per il recupero dell'account in caso di smarrimento del dispositivo MFA.
   e. Conserva la password in modo sicuro e considera le dipendenze circolari se la password viene conservata elettronicamente. Non memorizzare la password in modo tale da richiedere l'accesso allo stesso Account AWS per ottenerla.
6. Facoltativo: valuta la possibilità di stabilire un programma di rotazione periodica delle password per l'utente root.
   - Le best practice per la gestione delle credenziali dipendono dai requisiti normativi e di policy. Gli utenti root protetti da MFA non dipendono dalla password come unico fattore di autenticazione.
   - La modifica periodica della password dell'utente root riduce il rischio di utilizzo improprio di una password esposta inavvertitamente.

Controlli di rilevamento

- Crea allarmi per rilevare l'uso delle credenziali root (CIS 1.7). Amazon GuardDuty può monitorare e inviare avvisi sull'utilizzo delle credenziali API dell'utente root tramite l'esito RootCredentialUsage.
- Valuta e implementa i controlli investigativi inclusi nel pacchetto di conformità del pilastro della sicurezza AWS Well-Architected per AWS Config o, in caso di utilizzo di AWS Control Tower, i controlli fortemente consigliati disponibili in Control Tower.

Guida operativa

- Stabilisci chi nell'organizzazione deve avere accesso alle credenziali dell'utente root.
  - Utilizza una regola a due persone, in modo che nessun individuo abbia accesso a tutte le credenziali necessarie e all'MFA per ottenere l'accesso come utente root.
  - Verifica che l'organizzazione, e non un singolo individuo, mantenga il controllo sul numero di telefono e sull'alias e-mail associati all'account (utilizzati per il ripristino della password e il flusso di ripristino MFA).
- Utilizza l'utente root solo in via eccezionale (CIS 1.7).
  - L'utente root AWS non deve essere utilizzato per le attività giornaliere e nemmeno per quelle amministrative. Effettua l'accesso come utente root solo per eseguire attività AWS che richiedono l'utente root. Tutte le altre azioni devono essere eseguite da altri utenti che assumono i ruoli appropriati.
- Verifica periodicamente che l'accesso all'utente root sia funzionante, in modo da testare le procedure prima di una situazione di emergenza che richieda l'uso delle credenziali dell'utente root.
- Verifica a intervalli regolari il funzionamento dell'indirizzo e-mail associato all'account e quelli indicati nei contatti alternativi. Monitora queste caselle di posta elettronica per le notifiche di sicurezza che potresti ricevere da <abuse@amazon.com>. Assicurati inoltre che i numeri di telefono associati all'account siano attivi.
- Prepara procedure di risposta agli incidenti per rispondere all'uso improprio dell'account root. Consulta la AWS Security Incident Response Guide e le best practice nella sezione Risposta agli imprevisti del whitepaper sul pilastro della sicurezza per ulteriori informazioni circa la creazione di una strategia di risposta agli incidenti adatta al tuo Account AWS.

Risorse

Best practice correlate:

- SEC01-BP01 Separazione dei carichi di lavoro tramite account
- SEC02-BP01 Utilizzo di meccanismi di accesso efficaci
- SEC03-BP02 Concessione dell'accesso con privilegio minimo
- SEC03-BP03 Determinazione di un processo per l'accesso di emergenza
- SEC10-BP05 Preassegnazione dell'accesso

Documenti correlati:

- AWS Control Tower
- AWS Linee guida sugli audit di sicurezza
- Best practice di IAM
- Amazon GuardDuty: avviso di utilizzo delle credenziali root
- Step-by-step guidance on monitoring for root credential use through CloudTrail
- MFA tokens approved for use with AWS
- Implementazione di break glass access su AWS
- Top 10 security items to improve in your Account AWS
- What do I do if I notice unauthorized activity in my Account AWS?

Video correlati:

- Organizing Your AWS Environment Using Multiple Accounts
- Security Best Practices the Well-Architected Way
- Limitare l'uso delle credenziali root AWS da AWS re:inforce 2022 – Security best practices with AWS IAM

Gestione sicura dei carichi di lavoro

L'operatività dei carichi di lavoro include l'intero ciclo di vita di un carico di lavoro, dalla progettazione allo sviluppo, dall'esecuzione ai miglioramenti continui. Uno dei modi per migliorare la tua capacità di operare in sicurezza nel cloud è adottare un approccio organizzativo alla governance. La governance è alla base delle decisioni, che non dipendono solo dal buon senso delle persone coinvolte. Il modello e il processo di governance ti consentono di rispondere alla domanda "Come faccio a sapere se gli obiettivi di controllo per un dato carico di lavoro sono soddisfatti e adeguati per quel carico di lavoro?". Avere un approccio coerente alle decisioni velocizza l'implementazione dei carichi di lavoro e aiuta ad alzare il livello della sicurezza nella tua organizzazione.

Per gestire il carico di lavoro in modo sicuro, è necessario applicare le best practice globali a ogni area di sicurezza. Segui i requisiti e i processi definiti in termini di eccellenza operativa a livello organizzativo e di carico di lavoro e applicali a tutte le aree. Rimanere aggiornati con le raccomandazioni di AWS e del settore nonché con l'intelligence sulle minacce aiuta a sviluppare il modello di rischio e gli obiettivi di controllo. L'automazione dei processi di sicurezza, i test e la convalida consentono di scalare le operazioni di sicurezza.

L'automazione garantisce coerenza e ripetibilità dei processi. Le persone sono brave a fare molte cose, ma fare sempre la stessa attività in maniera ripetuta senza errori non è possibile. Anche con runbook scritti correttamente, corri il rischio che le persone non eseguano in modo coerente le attività ripetitive. Questo è soprattutto vero quando le persone hanno diverse responsabilità e devono quindi rispondere ad avvisi non noti. L'automazione, tuttavia, risponde sempre nello stesso modo. Il modo migliore per implementare le applicazioni è attraverso l'automazione. Il codice che esegue l'implementazione può essere testato e poi utilizzato per eseguire l'implementazione stessa. Questo aumenta la sicurezza nel processo di modifica e riduce il rischio di una modifica con esito negativo.

Per verificare che la configurazione soddisfi gli obiettivi di controllo, testa l'automazione e l'applicazione implementata prima in un ambiente non di produzione. In questo modo puoi testare l'automazione per dimostrare l'esecuzione corretta di tutti i passaggi. Puoi anche ottenere un feedback anticipato sullo sviluppo e il ciclo di implementazione, riducendo così un'eventuale rielaborazione. Per ridurre la possibilità di errori di implementazione, effettua le modifiche di configurazione tramite codice e non tramite le persone. Se hai bisogno di implementare nuovamente un'applicazione, l'automazione semplifica di molto questa operazione. Quando definisci obiettivi di controllo aggiuntivi, puoi facilmente aggiungerli all'automazione per tutti i carichi di lavoro.

Invece di avere proprietari dei singoli carichi di lavoro che investono aspetti della sicurezza specifici, risparmia tempo utilizzando funzionalità comuni e componenti condivisi. Alcuni esempi di servizi che più team possono usare includono il processo di creazione degli account AWS, l'identità centralizzata per le persone, la configurazione di creazione di log comuni e la creazione di immagini basate su container e AMI. Questo approccio può aiutare gli sviluppatori a migliorare i tempi del ciclo del carico di lavoro e soddisfare costantemente gli obiettivi dei controlli di sicurezza. Se i team sono più coerenti, puoi convalidare gli obiettivi di controllo e comunicare meglio la tua posizione di rischio e di controllo alle parti interessate.

Best practice

- SEC01-BP03 Identificazione e convalida degli obiettivi di controllo
- SEC01-BP04 Aggiornamento continuo sulle minacce alla sicurezza e sulle raccomandazioni
- SEC01-BP05 Riduzione dell'ambito di gestione della sicurezza
- SEC01-BP06 Implementazione automatizzata dei controlli di sicurezza standard
- SEC01-BP07 Identificare le minacce e dare priorità alle mitigazioni utilizzando un modello di minaccia.
- SEC01-BP08 Valutazione e implementazione periodiche di nuovi servizi e funzionalità di sicurezza

SEC01-BP03 Identificazione e convalida degli obiettivi di controllo

In base ai requisiti di conformità e ai rischi identificati dal modello di rischio, individua e convalida gli obiettivi di controllo e i controlli da applicare al carico di lavoro. La convalida continua degli obiettivi di controllo e dei controlli aiuta a misurare l'efficacia della mitigazione dei rischi.

Risultato desiderato: gli obiettivi di controllo della sicurezza della tua azienda sono ben definiti e in linea con i requisiti di conformità. I controlli vengono implementati e applicati attraverso l'automazione e le policy e vengono costantemente valutati per verificarne l'efficacia nel raggiungimento degli obiettivi. Le prove dell'efficacia, sia in un determinato momento che in un determinato periodo di tempo, sono prontamente comunicate ai revisori.

Anti-pattern comuni:

- I requisiti normativi, le aspettative del mercato e gli standard di settore per una sicurezza certa non sono ben compresi dalla tua azienda.
- I framework di sicurezza informatica e gli obiettivi di controllo non sono allineati ai requisiti dell'azienda.
- L'implementazione dei controlli non è perfettamente allineata agli obiettivi di controllo in modo misurabile.
- L'automazione non viene utilizzata per creare report sull'efficacia dei tuoi controlli.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

I framework di sicurezza informatica comunemente utilizzati sono molti e possono costituire la base per gli obiettivi di controllo della sicurezza. Per determinare quale sia il framework più adatto alle tue esigenze, considera i requisiti normativi, le aspettative del mercato e gli standard di settore dell'azienda. Tra gli esempi citiamo AICPA SOC 2, HITRUST, PCI-DSS, ISO 27.001 e NIST SP 800-53.

Per gli obiettivi di controllo identificati, occorre comprendere in che modo i servizi AWS utilizzati permettono di conseguirli. Utilizza AWS Artifact per individuare documentazione e report in linea con i tuoi framework di riferimento, che illustrino l'ambito di responsabilità coperto da AWS e linee guida per il restante ambito di tua responsabilità. Per ulteriori indicazioni specifiche sui servizi in linea con le varie dichiarazioni di controllo del framework, consulta le AWS Customer Compliance Guides.

Nel definire i controlli che raggiungono i tuoi obiettivi, codifica l'applicazione utilizzando i controlli preventivi e automatizza le mitigazioni mediante i controlli di rilevamento. Aiuta a prevenire configurazioni e azioni delle risorse non conformi su AWS Organizations mediante le policy di controllo dei servizi (SCP). Implementa le regole in AWS Config al fine di monitorare e segnalare le risorse non conformi, quindi passa a un modello di applicazione delle regole una volta che sei sicuro del loro comportamento. Per implementare set di regole predefinite e gestite in linea con i tuoi framework di sicurezza informatica, prendi in considerazione l'uso degli standard AWS Security Hub CSPM come prima opzione. Lo standard AWS Foundational Service Best Practices (FSBP) e il CIS AWS Foundations Benchmark sono validi punti di partenza con controlli che si allineano a molti obiettivi condivisi da più framework standard. Se Security Hub CSPM non dispone a livello intrinseco dei rilevamenti di controllo desiderati, è possibile integrarlo mediante i pacchetti di conformità AWS Config.

Utilizza i bundle dei partner APN consigliati dal team AWS Global Security and Compliance Acceleration (GSCA) per ottenere assistenza da consulenti di sicurezza, agenzie di consulenza, sistemi di raccolta e di reporting delle prove, revisori e altri servizi complementari, se necessario.

Passaggi dell'implementazione

1. Valuta i framework di sicurezza informatica comuni e allinea i tuoi obiettivi di controllo a quelli scelti.
2. Ottieni la documentazione pertinente sulle linee guida e le responsabilità per il tuo framework utilizzando AWS Artifact. Comprendi quali parti della conformità rientrano nel modello di responsabilità condivisa AWS e quali sono di tua competenza.
3. Utilizza le policy di controllo dei servizi, le policy sulle risorse, le policy di attendibilità dei ruoli e altri guardrail per prevenire configurazioni e azioni delle risorse non conformi.
4. Valuta l'implementazione di standard Security Hub CSPM e pacchetti di conformità AWS Config in linea con i tuoi obiettivi di controllo.

Risorse

Best practice correlate:

- SEC03-BP01 Definizione dei requisiti di accesso
- SEC04-BP01 Configurazione dei log di servizi e applicazioni
- SEC07-BP01 Comprendere lo schema di classificazione dei dati
- OPS01-BP03 Valutazione dei requisiti di governance

- OPS01-BP04 Valutazione dei requisiti di conformità
- PERF01-BP05 Uso delle policy e delle architetture di riferimento
- COST02-BP01 Sviluppo di policy basate sui requisiti dell'organizzazione

Documenti correlati:

- AWS Customer Compliance Guides

Strumenti correlati:

- AWS Artifact

SEC01-BP04 Aggiornamento continuo sulle minacce alla sicurezza e sulle raccomandazioni

Rimani aggiornato sulle minacce più recenti e sulle misure di mitigazione monitorando le pubblicazioni di intelligence sulle minacce del settore e i feed di dati per gli aggiornamenti. Valuta le offerte di servizi gestiti che si aggiornano in automatico in base ai dati sulle minacce più recenti.

Risultato desiderato: rimani informato mentre le pubblicazioni di settore si aggiornano con le ultime minacce e raccomandazioni. L'automazione viene utilizzata per rilevare potenziali vulnerabilità ed esposizioni man mano che si identificano nuove minacce. Intraprendi azioni di mitigazione contro queste minacce. Adotta servizi AWS che si aggiornano automaticamente con le informazioni sulle minacce più recenti.

Anti-pattern comuni:

- Non disporre di un meccanismo affidabile e ripetibile per rimanere informati sulle ultime informazioni sulle minacce.
- Mantenere un inventario manuale del portafoglio tecnologico, dei carichi di lavoro e delle dipendenze che richiedono un esame umano per individuare potenziali vulnerabilità ed esposizioni.
- Non disporre di meccanismi per aggiornare i carichi di lavoro e le dipendenze alle ultime versioni disponibili, che forniscono mitigazioni note delle minacce.

Vantaggi dell'adozione di questa best practice: l'utilizzo di fonti di intelligence sulle minacce per rimanere aggiornati riduce il rischio di lasciarsi sfuggire importanti cambiamenti nel panorama delle

minacce in grado di pregiudicare la tua azienda. L'automazione in atto per scansionare, rilevare e correggere eventuali vulnerabilità o esposizioni nei carichi di lavoro e nelle relative dipendenze può aiutarti a mitigare i rischi in modo rapido e prevedibile, rispetto alle alternative manuali. In questo modo puoi controllare i tempi e i costi relativi alla mitigazione delle vulnerabilità.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Consulta le pubblicazioni di intelligence sulle minacce per costanti aggiornamenti sul panorama delle minacce. Consulta la knowledge base MITRE ATT&CK per documentazione su tattiche, tecniche e procedure avversarie (TTP) note. Consulta l'elenco delle vulnerabilità e delle esposizioni comuni (CVE) di MITRE per non perdere gli aggiornamenti sulle vulnerabilità note nei prodotti su cui fai affidamento. Analizza i rischi critici per le applicazioni Web grazie al popolare progetto OWASP Top 10 di Open Worldwide Application Security Project (OWASP).

Non perdere gli ultimi aggiornamenti sugli eventi di sicurezza AWS e sulle procedure di correzione consigliate con i bollettini sulla sicurezza AWS per le CVE.

Per ridurre gli sforzi complessivi e il sovraccarico per rimanere aggiornati, valuta la possibilità di utilizzare i servizi AWS che incorporano automaticamente nuove informazioni sulle minacce nel tempo. Ad esempio, Amazon GuardDuty rimane aggiornato grazie all'intelligence sulle minacce di settore in modo da rilevare comportamenti anomali e firme di minacce all'interno dei tuoi account. Amazon Inspector mantiene in automatico aggiornato un database dei CVE che utilizza per le sue funzionalità di scansione continua. AWS WAF e AWS Shield Advanced forniscono gruppi di regole gestiti, aggiornati in automatico all'emergere di nuove minacce.

Esamina il pilastro dell'eccellenza operativa Well-Architected per la gestione e l'applicazione di patch automatizzate del parco.

Passaggi dell'implementazione

- Abbonati agli aggiornamenti per le pubblicazioni di intelligence sulle minacce pertinenti alla tua azienda e al tuo settore. Abbonati ai bollettini sulla sicurezza AWS.
- Prendi in considerazione l'adozione di servizi che incorporino automaticamente nuove informazioni sulle minacce, come Amazon GuardDuty e Amazon Inspector.
- Implementa una strategia di gestione e applicazione delle patch del parco in linea con le best practice del pilastro dell'eccellenza operativa Well-Architected.

Risorse

Best practice correlate:

- SEC01-BP07 Identificare le minacce e dare priorità alle mitigazioni utilizzando un modello di minaccia
- OPS01-BP05 Valutazione del panorama delle minacce
- OPS11-BP01 Definizione di un processo per il miglioramento continuo

SEC01-BP05 Riduzione dell'ambito di gestione della sicurezza

Stabilisci se sei in grado di ridurre l'ambito della sicurezza mediante servizi AWS che trasferiscono la gestione di determinati controlli su AWS (servizi gestiti). Questi servizi possono contribuire a ridurre le attività di manutenzione della sicurezza, come il provisioning dell'infrastruttura, l'impostazione del software, il patching o i backup.

Risultato desiderato: quando selezioni i servizi AWS per il carico di lavoro, prendi in considerazione l'ambito della gestione della sicurezza. Il costo delle spese generali di gestione e delle attività di manutenzione (il costo totale di proprietà o TCO) viene confrontato con il costo dei servizi selezionati, oltre ad altre considerazioni Well-Architected. La documentazione di controllo e conformità AWS viene incorporata nelle procedure di valutazione e verifica dei controlli.

Anti-pattern comuni:

- Implementazione dei carichi di lavoro senza comprendere a fondo il modello di responsabilità condivisa per i servizi selezionati.
- Hosting di database e altre tecnologie su macchine virtuali senza aver valutato un servizio gestito equivalente.
- Mancata inclusione delle attività di gestione della sicurezza nel costo totale di proprietà delle tecnologie di hosting su macchine virtuali rispetto alle opzioni di servizio gestito.

Vantaggi dell'adozione di questa best practice: l'utilizzo di servizi gestiti può ridurre l'onere complessivo della gestione dei controlli operativi della sicurezza, così da ridurre rischi per la sicurezza e costo totale di proprietà. Il tempo che altrimenti sarebbe dedicato a determinate attività di sicurezza può essere reinvestito in attività che forniscono maggior valore alla tua azienda. I servizi gestiti possono anche ridurre l'ambito dei requisiti di conformità spostando alcuni requisiti di controllo su AWS.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

Le modalità di integrazione dei componenti del carico di lavoro su AWS sono molteplici. L'installazione e l'esecuzione di tecnologie sulle istanze Amazon EC2 impongono spesso all'utente di assumersi la maggior parte delle responsabilità in materia di sicurezza. Per ridurre l'onere della gestione di alcuni controlli, individua i servizi gestiti AWS in grado di ridurre l'ambito della tua parte del modello di responsabilità condivisa e cerca di capire come utilizzarli nell'architettura esistente. Tra gli esempi citiamo l'utilizzo di Amazon Relational Database Service (Amazon RDS) per l'implementazione di database, Amazon Elastic Kubernetes Service (Amazon EKS) o Amazon Elastic Container Service (Amazon ECS) per l'orchestrazione di container o l'utilizzo di opzioni serverless. Quando sviluppi nuove applicazioni, pensa a quali servizi possono contribuire a ridurre i tempi e i costi di implementazione e gestione dei controlli di sicurezza.

Anche i requisiti di conformità possono essere un fattore di scelta dei servizi. I servizi gestiti possono trasferire la conformità di alcuni requisiti ad AWS. Discuti con il tuo team di conformità riguardo al loro livello di familiarità nel sottoporre ad audit gli aspetti dei servizi che gestisci e nell'accettare le dichiarazioni di controllo nei relativi report di audit di AWS. Puoi fornire gli artefatti di audit rilevati in AWS Artifact ai revisori o alle autorità di regolamentazione come prova dei controlli di sicurezza AWS. Puoi inoltre ricorrere alle linee guida sulla responsabilità fornite da alcuni degli artefatti di audit AWS per progettare la tua architettura, oltre alle AWS Customer Compliance Guides. Queste indicazioni aiutano a determinare i controlli di sicurezza aggiuntivi da mettere in atto per supportare i casi d'uso specifici del sistema.

Quando utilizzi servizi gestiti, è bene conoscere il processo di aggiornamento delle loro risorse a versioni più recenti (ad esempio, l'aggiornamento della versione di un database gestito da Amazon RDS o del runtime del linguaggio di programmazione per una funzione AWS Lambda). Anche se il servizio gestito può eseguire questa operazione per tuo conto, la configurazione della tempistica dell'aggiornamento e la conoscenza dell'impatto sulle tue operazioni restano di tua responsabilità. Strumenti come AWS Health ti consentono di tracciare e gestire questi aggiornamenti in tutti i tuoi ambienti.

Passaggi dell'implementazione

1. Valuta i componenti del tuo carico di lavoro sostituibili con un servizio gestito.
    a. Se stai migrando un carico di lavoro ad AWS, considera la riduzione della gestione (tempo e spese) e la conseguente diminuzione del rischio quando valuti l'opportunità di rehosting,

rifattorizzare, ridefinire la piattaforma, ricostruire o sostituire il carico di lavoro. A volte un investimento aggiuntivo all'inizio di una migrazione può comportare risparmi significativi nel lungo periodo.

2. Prendi in considerazione l'implementazione di servizi gestiti, come Amazon RDS, invece di installare e gestire le tue implementazioni tecnologiche.
3. Utilizza le linee guida sulla responsabilità in AWS Artifact per definire i controlli di sicurezza da adottare per il tuo carico di lavoro.
4. Tieni un inventario delle risorse in uso e rimani aggiornato con nuovi servizi e approcci per identificare nuove opportunità per ridurre l'ambito.

Risorse

Best practice correlate:

- PERF02-BP01 Selezione delle migliori opzioni di elaborazione per il carico di lavoro
- PERF03-BP01 Uso di un archivio dati dedicato che supporta al meglio i requisiti di accesso e archiviazione dei dati
- SUS05-BP03 Utilizzo dei servizi gestiti

Documenti correlati:

- Planned lifecycle events for AWS Health

Strumenti correlati:

- AWS Health
- AWS Artifact
- AWS Customer Compliance Guides

Video correlati:

- How do I migrate to an Amazon RDS or Aurora MySQL DB instance using AWS DMS?
- AWS re:Invent 2023 - Manage resource lifecycle events at scale with AWS Health

SEC01-BP06 Implementazione automatizzata dei controlli di sicurezza standard

Applica pratiche DevOps moderne mentre sviluppi e implementi controlli di sicurezza standard in tutti i tuoi ambienti AWS. Definisci controlli e configurazioni di sicurezza standard utilizzando i modelli Infrastructure as Code (IaC), acquisisci le modifiche in un sistema di controllo della versione, testa le modifiche come parte di una pipeline CI/CD e automatizza l'implementazione delle modifiche nei tuoi ambienti AWS.

Risultato desiderato: i modelli IaC acquisiscono controlli di sicurezza standardizzati, inserendoli in un sistema di controllo delle versioni. Le pipeline CI/CD si trovano in luoghi che rilevano le modifiche e automatizzano i test e l'implementazione degli ambienti AWS. Sono presenti guardrail per rilevare e fornire avvisi in caso di configurazioni errate nei modelli prima di procedere all'implementazione. I carichi di lavoro vengono implementati in ambienti dotati di controlli standard. I team hanno accesso all'implementazione di configurazioni di servizio approvate tramite un meccanismo self-service. Sono disponibili strategie di backup e ripristino sicure per le configurazioni di controllo, gli script e i dati correlati.

Anti-pattern comuni:

- Apportare modifiche ai controlli di sicurezza standard manualmente, tramite una console Web o un'interfaccia a riga di comando.
- Affidarsi ai singoli team del carico di lavoro per implementare manualmente i controlli definiti da un team centrale.
- Affidarsi a un team di sicurezza centrale per implementare i controlli a livello di carico di lavoro su richiesta di un team del carico di lavoro.
- Consentire agli stessi individui o team di sviluppare, testare e implementare script di automazione per il controllo della sicurezza senza un'adeguata separazione dei compiti o dei controlli e degli equilibri.

Vantaggi dell'adozione di questa best practice: l'utilizzo di modelli per definire i controlli di sicurezza standard consente di tracciare e confrontare le modifiche nel tempo con un sistema di controllo delle versioni. L'uso dell'automazione per testare e implementare le modifiche crea standardizzazione e prevedibilità, aumentando le possibilità di una corretta implementazione e riducendo le attività manuali ripetitive. Fornire un meccanismo self-service per consentire ai team addetti al carico di lavoro di implementare servizi e configurazioni approvati riduce il rischio di configurazioni errate e usi impropri. Questo li aiuta anche a incorporare i controlli nelle prime fasi del processo di sviluppo.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

Se segui le pratiche illustrate in SEC01-BP01 Separazione dei carichi di lavoro tramite account, avrai più Account AWS per diversi ambienti da gestire mediante AWS Organizations. Sebbene ciascuno di questi ambienti e carichi di lavoro possa richiedere controlli di sicurezza distinti, puoi standardizzarne alcuni in tutta l'organizzazione. Gli esempi includono l'integrazione di gestori dell'identità digitale centralizzati, la definizione di reti e firewall e la configurazione di posizioni standard per l'archiviazione e l'analisi dei log. Allo stesso modo in cui puoi utilizzare infrastructure as code (IaC) per applicare lo stesso criterio dello sviluppo del codice dell'applicazione al provisioning dell'infrastruttura, puoi usare l'IaC anche per definire e implementare controlli di sicurezza standard.

Se possibile, definisci i controlli di sicurezza in modo dichiarativo, ad esempio in AWS CloudFormation, e archiviali in un sistema di controllo del codice sorgente. Utilizza le pratiche DevOps per automatizzare l'implementazione dei controlli per versioni più prevedibili, test automatizzati mediante strumenti come AWS CloudFormation Guard e per il rilevamento della deviazione tra i controlli implementati e la configurazione desiderata. Puoi utilizzare servizi come AWS CodePipeline, AWS CodeBuild e AWS CodeDeploy per creare una pipeline CI/CD. Prendi in considerazione le linee guida in Organizing Your AWS Environment Using Multiple Accounts per configurare questi servizi negli account, separati dalle altre pipeline di implementazione.

Puoi inoltre definire modelli per standardizzare la definizione e l'implementazione di Account AWS, servizi e configurazioni. Questa tecnica consente a un team di sicurezza centrale di gestire queste definizioni e di fornirle ai team che si occupano dei carichi di lavoro attraverso un approccio self-service. Un modo per raggiungere questo obiettivo è utilizzare Service Catalog, dove è possibile pubblicare modelli come prodotti che i team addetti al carico di lavoro possono integrare nelle proprie implementazioni della pipeline. AWS Control Tower offre alcuni modelli e controlli come punto di partenza. Control Tower offre anche la funzionalità Account Factory, che consente ai team addetti al carico di lavoro di creare di nuovi Account AWS mediante gli standard definiti da te. Questa funzionalità aiuta a rimuovere le dipendenze da un team centrale per l'approvazione e la creazione di nuovi account quando vengono identificati come necessari dai team del carico di lavoro. Potresti aver bisogno di questi account per isolare i diversi componenti del carico di lavoro in base a motivi quali la funzione che svolgono, la sensibilità dei dati elaborati o il loro comportamento.

Passaggi dell'implementazione

1. Determina come archivierai e manterrai i tuoi modelli in un sistema di controllo delle versioni.

2. Crea pipeline CI/CD per testare e implementare i tuoi modelli. Definisci i test per verificare che non ci siano configurazioni errate e che i modelli siano conformi agli standard aziendali.
3. Crea un catalogo di modelli standardizzati affinché i team addetti al carico di lavoro possano implementare Account AWS e fornire servizi in base alle tue esigenze.
4. Implementa strategie di backup e ripristino sicure per le configurazioni di controllo, gli script e i dati correlati.

Risorse

Best practice correlate:

- OPS05-BP01 Utilizzo del controllo delle versioni
- OPS05-BP04 Utilizzo di sistemi di gestione della compilazione e implementazione
- REL08-BP05 Implementazione delle modifiche tramite automazione
- SUS06-BP01 Adozione di metodi che consentano di introdurre rapidamente migliorie in tema di sostenibilità

Documenti correlati:

- Organizzazione dell'ambiente AWS che utilizza più account

Esempi correlati:

- Automate account creation, and resource provisioning using Service Catalog, AWS Organizations, and AWS Lambda
- Strengthen the DevOps pipeline and protect data with Gestione dei segreti AWS, AWS KMS, and AWS Certificate Manager

Strumenti correlati:

- AWS CloudFormation Guard
- Landing Zone Accelerator on AWS

SEC01-BP07 Identificare le minacce e dare priorità alle mitigazioni utilizzando un modello di minaccia.

Effettua la modellazione delle minacce per identificare e mantenere un registro aggiornato delle minacce potenziali e delle relative mitigazioni per il carico di lavoro. Definisci le priorità delle minacce e adatta le mitigazioni dei controlli di sicurezza per prevenire, intercettare e rispondere. Riesamina e mantieni questo aspetto nel contesto del tuo carico di lavoro e dell'evoluzione del panorama della sicurezza.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Che cos'è la modellazione delle minacce?

"La modellazione delle minacce mira a identificare, comunicare e comprendere minacce e mitigazioni nel contesto della protezione di qualcosa di valore". – The Open Web Application Security Project (OWASP) Application Threat Modeling

Perché adottare la modellazione delle minacce?

I sistemi sono complessi, e nel tempo lo diventano sempre di più, e capaci di fornire un maggiore valore aziendale e una maggiore soddisfazione e coinvolgimento dei clienti. Ciò significa che le decisioni di progettazione IT devono tenere conto di un numero sempre maggiore di casi d'uso. Questa complessità e il numero di combinazioni di casi d'uso rendono in genere gli approcci non strutturati inefficaci per individuare e mitigare le minacce. È invece necessario un approccio sistematico per enumerare le potenziali minacce al sistema ed elaborare le mitigazioni, oltre che per stabilirne le priorità per assicurarsi che le risorse limitate dell'organizzazione abbiano il massimo impatto nel migliorare lo stato di sicurezza complessiva del sistema.

La modellazione delle minacce è progettata per offrire questo approccio sistematico, con l'obiettivo di trovare e affrontare i problemi nelle prime fasi del processo di progettazione, quando le mitigazioni hanno un costo e un impegno relativi bassi rispetto alle fasi successive del ciclo di vita. Questo approccio è in linea con il principio di sicurezza shift-left. In definitiva, la modellazione delle minacce si integra con il processo di gestione del rischio di un'organizzazione e aiuta a prendere decisioni sui controlli da implementare utilizzando un approccio orientato alle minacce.

Quando eseguire la modellazione delle minacce?

La modellazione delle minacce deve essere avviata il prima possibile nel ciclo di vita del carico di lavoro, in modo da avere una maggiore flessibilità di intervento sulle minacce identificate. Come per i bug del software, prima si identificano le minacce, più è conveniente affrontarle. Un modello di minacce è un documento vivo e deve continuare a evolvere in base ai cambiamenti dei carichi di lavoro. I modelli di minaccia vanno riesaminati nel tempo, anche in caso di modifiche importanti, di cambiamenti nel panorama delle minacce o di adozione di nuove funzionalità o servizi.

Passaggi dell'implementazione

In che modo è possibile eseguire la modellazione delle minacce?

Esistono diversi modi per eseguire la modellazione delle minacce. Come per i linguaggi di programmazione, anche in questo caso ci sono vantaggi e svantaggi e bisogna scegliere il metodo più adatto alle proprie esigenze. Un approccio consiste nell'iniziare con 4 domande per la modellazione delle minacce di Shostack, che pone domande aperte per fornire una struttura per il tuo esercizio di modellazione delle minacce:

1. A cosa si sta lavorando?

   Questa domanda ha lo scopo di aiutare a comprendere e concordare il sistema che si sta costruendo e i dettagli di tale sistema che sono rilevanti per la sicurezza. La creazione di un modello o di un diagramma è la soluzione più comune per rispondere a questa domanda, in quanto consente di visualizzare ciò che si sta creando, ad esempio utilizzando un diagramma di flusso dei dati. Scrivere ipotesi e dettagli importanti del sistema aiuta anche a definire l'ambito di applicazione. In questo modo, tutti coloro che contribuiscono alla modellazione delle minacce possono concentrarsi sullo stesso aspetto, evitando deviazioni dispendiose in termini di tempo su argomenti fuori portata (comprese le versioni non aggiornate del sistema). Ad esempio, se si sta realizzando un'applicazione Web, probabilmente non vale la pena procedere alla modellazione per la sequenza di avvio attendibile del sistema operativo per i browser client, poiché non si ha la possibilità di influire su questo aspetto con il proprio progetto.
2. Che cosa può andare storto?

   In questa fase si identificano le minacce al sistema. Le minacce sono azioni o eventi accidentali o intenzionali che producono impatti indesiderati e potrebbero compromettere la sicurezza del sistema. Senza una visione chiara di ciò che potrebbe andare storto, non è possibile fare nulla per evitarlo.

   Non esiste un elenco canonico di ciò che può andare storto. La creazione di questo elenco richiede un brainstorming e la collaborazione tra tutte le persone del team e le persone pertinenti

coinvolte nell'esercizio di modellazione delle minacce. Per semplificare il brainstorming, utilizza un modello per identificare le minacce, come STRIDE, che suggerisce diverse categorie da valutare: spoofing, manomissione, ripudio, divulgazione di informazioni, negazione del servizio ed elevazione dei privilegi. Inoltre, potresti contribuire al brainstorming consultando gli elenchi esistenti e traendone ispirazione, tra cui OWASP Top 10, HiTrust Threat Catalog e il catalogo delle minacce della tua organizzazione.

3. Cosa si intende fare al riguardo?

   Come nel caso della domanda precedente, non esiste un elenco canonico di tutte le possibili mitigazioni. Gli input di questa fase sono le minacce, gli attori e le aree di miglioramento identificate nella fase precedente.

   Sicurezza e conformità sono una responsabilità condivisa tra AWS e l'utente. È importante capire che quando si chiede "Che si farà al riguardo?", si chiede anche "Chi è responsabile? Chi ha la responsabilità di fare qualcosa?" Comprendere l'equilibrio delle responsabilità tra utente e AWS consente di limitare l'esercizio di modellazione delle minacce alle mitigazioni sotto il proprio controllo, che di solito sono una combinazione di opzioni di configurazione del servizio AWS e di mitigazioni specifiche del proprio sistema.

   In merito alla parte di responsabilità di AWS condivisa, scoprirai che i servizi AWS rientrano nell'ambito di molti programmi di conformità. Questi programmi aiutano a comprendere i solidi controlli in atto presso AWS per mantenere la sicurezza e la conformità del cloud. I report di audit di questi programmi possono essere scaricati per i clienti AWS da AWS Artifact.

   Indipendentemente dai servizi AWS utilizzati, c'è sempre una responsabilità del cliente e le mitigazioni allineate a tale responsabilità devono essere incluse nel modello di minaccia. Per quanto riguarda le mitigazioni dei controlli di sicurezza per i servizi AWS stessi, è necessario considerare l'implementazione dei controlli di sicurezza in tutti i domini, compresi quelli quali la gestione delle identità e degli accessi (autenticazione e autorizzazione), la protezione dei dati (a riposo e in transito), la sicurezza dell'infrastruttura, la creazione di log e il monitoraggio. La documentazione di ciascun servizio AWS prevede un capitolo dedicato alla sicurezza, con indicazioni sui controlli di sicurezza da prendere in considerazione come mitigazioni. È importante considerare il codice che si sta scrivendo e le sue dipendenze e pensare ai controlli attuabili per affrontare queste minacce. Questi controlli potrebbero corrispondere a elementi quali la convalida degli input, la gestione delle sessioni e la gestione dei limiti. Spesso la maggior parte delle vulnerabilità viene introdotta nel codice personalizzato, quindi è bene concentrarsi su quest'area.

4. È stato fatto un buon lavoro?

L'obiettivo è il miglioramento da parte del team e dell'organizzazione sia della qualità dei modelli di minacce sia della relativa velocità di esecuzione nel tempo. Questi miglioramenti derivano da una combinazione di pratica, apprendimento, insegnamento e revisione. Per approfondire e sperimentare nella pratica, è consigliabile che tu e il tuo team completiate il corso di formazione Threat modeling the right way for builders training course o il workshop. Inoltre, se stai cercando indicazioni su come integrare la modellazione delle minacce nel ciclo di vita di sviluppo delle applicazioni della tua organizzazione, consulta il post How to approach threat modeling sul blog di AWS sulla sicurezza.

Threat Composer

Come strumento di ausilio e guida nella modellazione delle minacce, prendi in considerazione l'utilizzo dello strumento Threat Composer, il cui scopo è ridurre il time-to-value di questa attività. Lo strumento consente di eseguire le seguenti operazioni:

- Scrivere dichiarazioni utili sulle minacce in linea con la sintassi delle minacce che funzionino in un flusso di lavoro naturale non lineare
- Generare un modello di minaccia leggibile dall'uomo
- Generare un modello di minaccia leggibile dal computer per consentire la gestione dei modelli di minaccia come codice
- Velocizzare l'individuazione delle aree di miglioramento della qualità e della copertura utilizzando l'area del pannello di controllo contenente le informazioni dettagliate

Per ulteriori informazioni, visita Threat Composer e passa all'area di lavoro esemplificativa definita dal sistema.

Risorse

Best practice correlate:

- SEC01-BP03 Identificazione e convalida degli obiettivi di controllo
- SEC01-BP04 Aggiornamento continuo sulle minacce alla sicurezza e sulle raccomandazioni
- SEC01-BP05 Riduzione dell'ambito di gestione della sicurezza
- SEC01-BP08 Valutazione e implementazione periodiche di nuovi servizi e funzionalità di sicurezza

Documenti correlati:

- Come approcciare la modellazione delle minacce (AWS Security Blog)
- NIST: Guide to Data-Centric System Threat modeling

Video correlati:

- AWS Summit ANZ 2021 - How to approach threat modelling
- AWS Summit ANZ 2022 - Scaling security – Optimise for fast and secure delivery

Formazione correlata:

- Threat modeling the right way for builders – AWS Skill Builder virtual self-paced training
- Threat modeling the right way for builders – AWS Workshop

Strumenti correlati:

- Threat Composer

SEC01-BP08 Valutazione e implementazione periodiche di nuovi servizi e funzionalità di sicurezza

Valuta e implementa servizi e funzionalità di sicurezza di AWS e partner AWS che consentano di sviluppare l'assetto di sicurezza del carico di lavoro.

Risultato desiderato: hai adottato una procedura standard che ti informa su nuovi servizi e funzionalità rilasciati da AWS e dai partner AWS. Puoi valutare come queste nuove funzionalità influenzino la progettazione di controlli attuali e nuovi per i tuoi ambienti e carichi di lavoro.

Anti-pattern comuni:

- Non ti iscrivi ai blog e ai feed RSS di AWS per conoscere rapidamente le nuove funzionalità e i servizi più importanti.
- Fai affidamento su notizie e aggiornamenti sui servizi e sulle funzioni di sicurezza provenienti da fonti di seconda mano
- Non incoraggi gli utenti AWS della tua organizzazione a rimanere informati sugli ultimi aggiornamenti

Vantaggi dell'adozione di questa best practice: rimanere aggiornati sui nuovi servizi e funzionalità di sicurezza, consente di adottare decisioni informate sull'implementazione dei controlli negli ambienti cloud e nei carichi di lavoro. Queste origini contribuiscono ad aumentare la consapevolezza dell'evoluzione del panorama della sicurezza e di come i servizi AWS possano essere utilizzati per proteggersi dalle minacce nuove ed emergenti.

Livello di rischio associato se questa best practice non fosse adottata: basso

Guida all'implementazione

AWS informa i clienti sui nuovi servizi e funzionalità di sicurezza attraverso diversi canali:

- AWS What's New
- AWS Blog delle novità
- AWS Security Blog
- AWS Security Bulletins
- AWS documentation overview

Puoi iscriverti a un argomento AWS Daily Feature Updates utilizzando Amazon Simple Notification Service (Amazon SNS) per un riepilogo giornaliero completo degli aggiornamenti. Alcuni servizi di sicurezza, come Amazon GuardDuty e AWS Security Hub CSPM, forniscono i propri argomenti SNS in modo da restare informati su nuovi standard, esiti e altri aggiornamenti di questi particolari servizi.

Anche durante conferenze, eventi e webinar che si tengono ogni anno in tutto il mondo, vengono annunciati nuovi servizi e funzionalità. Segnaliamo in particolare conferenza annuale sulla sicurezza AWS re:Inforce e la conferenza più generale AWS re:Invent. I canali di notizie AWS di cui sopra condividono questi annunci relativi a conferenze sulla sicurezza e su altri servizi. Inoltre, puoi guardare le sessioni breakout di approfondimento didattiche online sul canale AWS Events channel e su YouTube.

Puoi anche chiedere al team del tuo Account AWS informazioni sugli aggiornamenti e consigli più recenti sui servizi di sicurezza. Puoi contattare il team tramite il modulo Sales Support se non disponi dei loro recapiti diretti. Allo stesso modo, se sei abbonato al supporto AWS Enterprise, riceverai aggiornamenti settimanali dal tuo Technical Account Manager (TAM) e potrai programmare una riunione di revisione regolare con lo stesso.

Passaggi dell'implementazione

1. Iscriviti ai vari blog e bollettini con il tuo lettore RSS preferito o all'argomento Daily Features Updates SNS.
2. Valuta gli eventi AWS a cui partecipare per conoscere in prima persona nuove funzionalità e servizi.
3. Organizza riunioni con il team Account AWS per qualsiasi domanda sull'aggiornamento dei servizi e delle funzionalità di sicurezza.
4. Prendi in considerazione la possibilità di abbonarti a Enterprise Support per avere consulenze regolari con un Technical Account Manager (TAM).

Risorse

Best practice correlate:

- PERF01-BP01 Informazioni e identificazione dei servizi e delle funzionalità cloud disponibili
- COST01-BP07 Mantenimento dell'aggiornamento sulle nuove versioni dei servizi

Gestione dell'identità e degli accessi

Per utilizzare i servizi AWS, devi concedere agli utenti e alle applicazioni l'accesso alle risorse nei tuoi account AWS. Quando esegui più carichi di lavoro su AWS, hai bisogno di una solida gestione delle identità e delle autorizzazioni per garantire che le persone giuste abbiano accesso alle risorse corrette in condizioni appropriate. AWS offre un'ampia gamma di funzionalità per aiutarti a gestire le identità di persone e macchine e le relative autorizzazioni. Le best practice per queste funzionalità rientrano in due aree principali.

Argomenti

Gestione delle identità

Ci sono due tipi di identità da gestire quando inizi a utilizzare carichi di lavoro AWS sicuri.

- Identità umane: le identità umane che richiedono l'accesso agli ambienti e alle applicazioni AWS possono essere classificate in tre gruppi, ossia forza lavoro, terze parti e utenti.

  Il gruppo della forza lavoro include amministratori, sviluppatori e operatori che sono membri dell'organizzazione. Hanno bisogno dell'accesso per gestire, creare e utilizzare le risorse AWS.

  Il gruppo delle terze parti include collaboratori esterni, come appaltatori, fornitori o partner. Interagiscono con le risorse AWS nell'ambito del loro rapporto di lavoro con l'organizzazione.

  Il gruppo degli utenti include i consumatori delle applicazioni. Accedono alle risorse AWS tramite browser web, applicazioni client, app per dispositivi mobili o strumenti da riga di comando interattivi.
- Identità di macchine: le applicazioni per il carico di lavoro, gli strumenti operativi e i componenti necessitano di un'identità per effettuare richieste ai servizi AWS, ad esempio la lettura dei dati. Queste identità includono anche macchine in esecuzione all'interno dell'ambiente AWS, come le istanze Amazon EC2 o le funzioni AWS Lambda. Puoi anche gestire le identità di macchine per soggetti esterni, o per macchine al di fuori di AWS, che richiedono l'accesso all'ambiente AWS.

Best practice

- SEC02-BP01 Utilizzo di meccanismi di accesso efficaci
- SEC02-BP02 Utilizzo di credenziali temporanee
- SEC02-BP03 Archiviazione e utilizzo dei segreti in modo sicuro
- SEC02-BP04 Fai affidamento su un gestore dell'identità digitale centralizzato
- SEC02-BP05 Verifica e rotazione periodica delle credenziali
- SEC02-BP06 Impiego dei gruppi di utenti e degli attributi

SEC02-BP01 Utilizzo di meccanismi di accesso efficaci

Gli accessi (autenticazione tramite credenziali di accesso) possono presentare dei rischi se non si utilizzano meccanismi come l'autenticazione a più fattori (MFA), soprattutto in situazioni in cui le credenziali di accesso sono state inavvertitamente divulgate o sono facilmente identificabili. Utilizza meccanismi di accesso efficaci per ridurre tali rischi, richiedendo l'MFA e policy sulle password sicure.

Risultato desiderato: ridurre i rischi di accessi accidentali alle credenziali AWS utilizzando meccanismi di accesso avanzati per gli utenti AWS Identity and Access Management (IAM), l'utente root Account AWS, AWS IAM Identity Center e i gestori dell'identità digitale di terze parti. Ciò significa richiedere l'MFA, applicare policy sulle password efficaci e rilevare comportamenti di accesso anomali.

Anti-pattern comuni:

- Nessuna applicazione di policy sulle password efficaci per le proprie identità, comprese password complesse e MFA.
- Condivisione delle stesse credenziali tra utenti diversi.
- Nessun utilizzo di controlli investigativi per gli accessi sospetti.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Ci sono diversi modi in cui le identità umane possono accedere a AWS. È una best practice di AWS affidarsi a un gestore dell'identità digitale centralizzato utilizzando la federazione (federazione diretta SAML 2.0 tra AWS IAM e l'IdP centralizzato o utilizzando Centro identità AWS IAM) per

l'autenticazione ad AWS. In questo caso, stabilisci un processo di accesso sicuro con il gestore dell'identità digitale o con Microsoft Active Directory.

Quando apri un Account AWS, inizi con un utente root Account AWS. L'utente root dell'account va utilizzato solo per configurare l'accesso degli utenti (e per le attività che richiedono l'utente root). È importante attivare l'autenticazione a più fattori (MFA) per l'utente root dell'account subito dopo l'apertura dell'Account AWS e proteggere l'utente root utilizzando la guida alle best practice di AWS.

Centro identità AWS IAM è progettato per gli utenti della forza lavoro; puoi creare e gestire le identità degli utenti all'interno del servizio e proteggere il processo di accesso con l'MFA. AWS Cognito, invece, è progettato per la gestione di identità e accessi del cliente (CIAM), che fornisce pool di utenti e gestore dell'identità digitale per le identità degli utenti esterni nelle applicazioni.

Se crei utenti in Centro identità AWS IAM, proteggi il processo di accesso in tale servizio e attiva MFA. Per le identità degli utenti esterni nelle applicazioni, puoi utilizzare i pool di utenti di Amazon Cognito e proteggere il processo di accesso in tale servizio o attraverso uno dei gestori dell'identità digitale supportati nei pool di utenti di Amazon Cognito.

Inoltre, per gli utenti in Centro identità AWS IAM, puoi utilizzare Accesso verificato da AWS per fornire un ulteriore livello di sicurezza, verificando l'identità e la postura del dispositivo dell'utente prima che venga concesso l'accesso alle risorse AWS.

Se utilizzi utenti AWS Identity and Access Management (IAM), proteggi il processo di accesso utilizzando IAM.

Puoi utilizzare contemporaneamente Centro identità AWS IAM e federazione diretta IAM per gestire l'accesso ad AWS. Puoi utilizzare la federazione IAM per gestire l'accesso a Console di gestione AWS e ai servizi e Centro identità IAM per gestire l'accesso ad applicazioni aziendali come Quick o Amazon Q Business.

Indipendentemente dal metodo di accesso, è fondamentale applicare una policy di accesso efficace.

Passaggi dell'implementazione

Di seguito sono indicate raccomandazioni generali per l'accesso sicuro. Configura le impostazioni effettive in base alla policy aziendale. In alternativa, utilizza uno standard, come NIST 800-63.

- Richiedi MFA. È una best practice IAM richiedere l'MFA per identità umane e carichi di lavoro. L'attivazione dell'MFA fornisce un ulteriore livello di sicurezza che richiede agli utenti di fornire le credenziali di accesso e un codice OTP (One-Time Password) o una stringa verificata e generata a livello crittografico da un dispositivo hardware.

- Applica una lunghezza minima della password, fattore primario nell'efficacia della password.
- Applica la complessità delle password in modo che sia più difficile individuarle.
- Consenti agli utenti di cambiare le loro password.
- Crea identità individuali invece di credenziali condivise. Creando identità individuali, puoi assegnare a ciascun utente un set unico di credenziali di sicurezza. I singoli utenti consentono di sottoporre ad audit l'attività di ciascuno.

Consigli del Centro identità IAM:

- Il Centro identità IAM offre una policy sulle password prestabilita in caso di utilizzo della directory predefinita che stabilisce lunghezza, complessità e requisiti di riutilizzo della password.
- Attiva l'MFA e configura l'impostazione relativa alla sensibilità al contesto o all'attivazione costante per l'MFA quando l'origine di identità è la directory predefinita, AWS Managed Microsoft AD o AD Connector.
- Consenti agli utenti di registrare i propri dispositivi MFA.

Consigli sulle directory dei pool di utenti Amazon Cognito:

- Configura le impostazioni relative alla complessità della password.
- Richiedi l'MFA per gli utenti.
- Le impostazioni di sicurezza avanzate dei pool di utenti di Amazon Cognito offrono funzionalità come l'autenticazione adattiva, che può bloccare gli accessi sospetti.

Suggerimenti per l'utente IAM:

- Idealmente stai utilizzando il Centro identità IAM o la federazione diretta. Tuttavia, potrebbero essere necessari utenti IAM. In tal caso, imposta una policy sulle password per gli utenti IAM. Puoi utilizzare la policy sulle password per definire requisiti quali la lunghezza minima o la necessità che la password richieda caratteri non alfabetici.
- Crea una policy IAM per applicare l'accesso MFA: in questo modo, gli utenti potranno gestire le proprie password e i propri dispositivi MFA.

Risorse

Best practice correlate:

- SEC02-BP03 Archiviazione e utilizzo dei segreti in modo sicuro
- SEC02-BP04 Fai affidamento su un gestore dell'identità digitale centralizzato
- SEC03-BP08 Condivisione delle risorse in modo sicuro all'interno dell'organizzazione

Documenti correlati:

- AWS IAM Identity Center Password Policy
- IAM user password policy
- Setting the Account AWS root user password
- Amazon Cognito password policy
- AWS credentials
- IAM security best practices

Video correlati:

- Managing user permissions at scale with AWS IAM Identity Center
- Mastering identity at every layer of the cake

SEC02-BP02 Utilizzo di credenziali temporanee

Quando si esegue qualsiasi tipo di autenticazione, è preferibile utilizzare credenziali temporanee invece di credenziali a lungo termine per ridurre o eliminare i rischi, come la divulgazione, la condivisione o il furto involontario delle stesse.

Risultato desiderato: al fine di ridurre il rischio di credenziali a lungo termine, utilizza credenziali temporanee laddove possibile per le identità di persone e macchine. Le credenziali a lungo termine creano molti rischi, come l'esposizione attraverso i caricamenti su repository pubblici. Grazie alle credenziali temporanee, riduci notevolmente le possibilità di compromissione delle credenziali.

Anti-pattern comuni:

- Sviluppatori che utilizzano chiavi di accesso a lungo termine dagli utenti IAM anziché ottenere credenziali temporanee dalla CLI utilizzando la federazione.
- Sviluppatori che inseriscono chiavi di accesso a lungo termine nel loro codice e caricano tale codice su repository Git pubblici.

- Sviluppatori che inseriscono chiavi di accesso a lungo termine nelle app mobili che vengono poi rese disponibili negli app store.
- Utenti che condividono le chiavi di accesso a lungo termine con altri utenti o dipendenti che lasciano l'azienda con chiavi di accesso a lungo termine ancora in loro possesso.
- Utilizzo di chiavi di accesso a lungo termine per le identità macchina quando è possibile utilizzare credenziali temporanee.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Utilizza credenziali di sicurezza temporanee anziché credenziali a lungo termine per tutte le richieste API e CLI AWS. In quasi tutti i casi, le richieste API e CLI rivolte ai servizi AWS devono essere firmate mediante chiavi di accesso AWS. Queste richieste possono essere firmate con credenziali temporanee o a lungo termine. L'unico caso in cui occorre utilizzare credenziali a lungo termine, note anche come chiavi di accesso a lungo termine, è l'utilizzo di utenti IAM o dell'utente root Account AWS. L'utilizzo della federazione per AWS o l'assunzione di un ruolo IAM tramite altri metodi prevede la creazione di credenziali temporanee. Anche quando accedi a Console di gestione AWS utilizzando le credenziali di accesso, vengono generate credenziali temporanee per effettuare chiamate ai servizi AWS. Sono poche le situazioni in cui occorrono credenziali a lungo termine ed è possibile svolgere quasi tutte le attività utilizzando credenziali temporanee.

Evitare l'uso di credenziali a lungo termine a favore di credenziali temporanee dovrebbe andare di pari passo con una strategia di riduzione dell'uso degli utenti IAM a favore della federazione e dei ruoli IAM. Sebbene l'utilizzo in passato degli utenti IAM sia per le identità umane che per quelle macchina, ora si consiglia di non utilizzarli per evitare i rischi legati all'uso di chiavi di accesso a lungo termine.

Passaggi dell'implementazione

Identità umane

Per le identità della forza lavoro come dipendenti, amministratori, sviluppatori e operatori:

- Dovresti affidarti a gestori dell'identità digitale centralizzati e richiedere agli utenti umani di utilizzare la federazione con un gestore dell'identità digitale per accedere ad AWS utilizzando credenziali temporanee. La federazione per gli utenti può essere effettuata sia con la federazione diretta a ciascun Account AWS sia utilizzando Centro identità AWS IAM e il gestore dell'identità digitale preferito. La federazione offre una serie di vantaggi rispetto all'utilizzo degli utenti IAM, oltre

all'eliminazione delle credenziali a lungo termine. I tuoi utenti possono inoltre richiedere credenziali temporanee dalla riga di comando per la federazione diretta o utilizzando il Centro identità IAM. Ciò significa che i casi d'uso che richiedono utenti IAM o credenziali a lungo termine per gli utenti sono pochi.

Per le identità di terze parti:

- Quando concedi l'accesso alle risorse del tuo Account AWS a terze parti, come i fornitori di software as a service (SaaS), puoi utilizzare ruoli multi-account e policy basate su risorse. Inoltre, puoi utilizzare il flusso delle credenziali client di concessione di Amazon Cognito OAuth 2.0 per clienti o partner SaaS B2B.

Identità utente che accedono alle risorse AWS tramite browser web, applicazioni client, app per dispositivi mobili o strumenti interattivi da riga di comando:

- Se devi concedere alle applicazioni per consumatori o clienti l'accesso alle tue risorse AWS, puoi utilizzare i pool di identità di Amazon Cognito o i pool di utenti Amazon Cognito per fornire credenziali temporanee. Le autorizzazioni per le credenziali sono configurate attraverso i ruoli IAM. Puoi inoltre definire un ruolo IAM separato con autorizzazioni limitate per gli utenti guest non autenticati.

Identità macchina

Per le identità macchina, potrebbero essere necessarie credenziali a lungo termine. In questi casi, dovresti richiedere ai carichi di lavoro di utilizzare credenziali temporanee con ruoli IAM per l'accesso ad AWS.

- Per Amazon Elastic Compute Cloud (Amazon EC2), puoi utilizzare i ruoli per Amazon EC2.
- AWS Lambda ti consente di configurare un ruolo di esecuzione Lambda per la concessione delle autorizzazioni di servizio al fine di eseguire azioni AWS mediante credenziali temporanee. Per i servizi AWS esistono molti altri modelli simili per concedere credenziali temporanee utilizzando i ruoli IAM.
- Per i dispositivi IoT, puoi richiedere credenziali temporanee al provider di credenziali AWS IoT Core.
- Per sistemi on-premises o quelli eseguiti all'esterno di AWS che richiedono l'accesso alle risorse AWS, puoi utilizzare IAM Roles Anywhere.

Esistono scenari in cui le credenziali temporanee non sono supportate e che richiedono l'uso di credenziali a lungo termine. In queste situazioni, verifica e ruota periodicamente queste credenziali e ruota regolarmente le chiavi di accesso. Per chiavi di accesso dell'utente IAM altamente limitate, considera le seguenti misure di sicurezza aggiuntive:

- Concedi autorizzazioni altamente limitate:
  - Rispetta il principio del privilegio minimo (con impostazioni specifiche per azioni, risorse e condizioni).
  - Valuta la possibilità di concedere all'utente IAM solo l'operazione AssumeRole per un ruolo specifico. A seconda dell'architettura on-premises, questo approccio consente di isolare e proteggere le credenziali IAM a lungo termine.
- Limita le origini della rete e gli indirizzi IP consentiti nella policy di attendibilità dei ruoli IAM.
- Monitora l'utilizzo e imposta avvisi per le autorizzazioni non utilizzate o l'uso improprio (utilizzando i filtri metriche e gli allarmi di AWS CloudWatch Logs).
- Applica i limiti delle autorizzazioni (le policy di controllo dei servizi (SCP) e i limiti delle autorizzazioni si completano a vicenda: le SCP sono poco granulari, mentre i limiti delle autorizzazioni sono più granulari).
- Implementa un processo per il provisioning e l'archiviazione sicura (in vault on-premises) delle credenziali.

Altre opzioni per gli scenari che richiedono credenziali a lungo termine sono le seguenti:

- Crea la tua API di distribuzione di token (utilizzando Gateway Amazon API).
- Per gli scenari in cui è necessario utilizzare credenziali a lungo termine o credenziali diverse dalle chiavi di accesso AWS (come i login ai database), puoi utilizzare un servizio progettato per gestire i segreti, come Gestione dei segreti AWS. Secrets Manager semplifica la gestione, la rotazione e l'archiviazione sicura dei segreti crittografati. Molti servizi AWS supportano l'integrazione diretta con Secrets Manager.
- Per le integrazioni multi-cloud, puoi utilizzare la federazione delle identità basata sulle credenziali del provider di servizi di credenziali (CSP) di origine (consulta AWS STS AssumeRoleWithWebIdentity).

Per ulteriori informazioni sulla rotazione delle credenziali a lungo termine, consulta rotazione delle chiavi di accesso.

Risorse

Best practice correlate:

- SEC02-BP03 Archiviazione e utilizzo dei segreti in modo sicuro
- SEC02-BP04 Fai affidamento su un gestore dell'identità digitale centralizzato
- SEC03-BP08 Condivisione delle risorse in modo sicuro all'interno dell'organizzazione

Documenti correlati:

- Temporary Security Credentials
- AWS Credenziali
- IAM Security Best Practices
- Ruoli IAM
- Centro identità IAM
- Identity Providers and Federation
- Rotating Access Keys
- Soluzioni dei partner per la sicurezza: accesso e controllo degli accessi
- L'utente root dell'account AWS
- Access AWS using a Google Cloud Platform native workload identity
- How to access AWS resources from Microsoft Entra ID tenants using AWS Security Token Service

Video correlati:

- Managing user permissions at scale with AWS IAM Identity Center
- Mastering identity at every layer of the cake

SEC02-BP03 Archiviazione e utilizzo dei segreti in modo sicuro

Un carico di lavoro richiede una capacità automatizzata di dimostrare la propria identità a database, risorse e servizi di terze parti. A tal fine, si utilizzano credenziali di accesso segrete, come chiavi di accesso API, password e token OAuth. L'utilizzo di un servizio appositamente creato per archiviare, gestire e ruotare queste credenziali aiuta a ridurre la probabilità che queste vengano compromesse.

Risultato desiderato: implementazione di un meccanismo per la gestione sicura delle credenziali delle applicazioni che consenta di raggiungere i seguenti obiettivi.

- Identificare i segreti necessari per il carico di lavoro.
- Ridurre il numero di credenziali a lungo termine sostituendole con credenziali a breve termine, laddove possibile.
- Stabilire l'archiviazione sicura e la rotazione automatica delle rimanenti credenziali a lungo termine.
- Sottoporre a audit l'accesso ai segreti esistenti nel carico di lavoro.
- Eseguire il monitoraggio continuo per verificare che nessun segreto sia incorporato nel codice sorgente durante il processo di sviluppo.
- Ridurre la probabilità che le credenziali vengano divulgate inavvertitamente.

Anti-pattern comuni:

- Nessuna rotazione delle credenziali.
- Memorizzazione di credenziali a lungo termine nel codice sorgente o nei file di configurazione.
- Memorizzazione delle credenziali a riposo non criptate.

Vantaggi dell'adozione di questa best practice:

- I segreti sono conservati in modo criptato a riposo e in transito.
- L'accesso alle credenziali è controllato tramite un'API (immaginala come un distributore automatico di credenziali).
- L'accesso alle credenziali (sia in lettura che in scrittura) viene sottoposto a audit e registrato.
- Separazione delle preoccupazioni: la rotazione delle credenziali viene eseguita da un componente distinto, che può essere segregato dal resto dell'architettura.
- La distribuzione dei segreti avviene in automatico on demand ai componenti software e la rotazione avviene in una posizione centrale.
- È possibile controllare l'accesso alle credenziali in modo granulare.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

In passato, le credenziali utilizzate per l'autenticazione ai database, alle API di terze parti, ai token e ad altri segreti potevano essere incorporate nel codice sorgente o nei file di ambiente. AWS fornisce diversi meccanismi per memorizzare queste credenziali in modo sicuro, ruotarle in automatico e sottoporre a audit il loro utilizzo.

Il modo migliore per affrontare la gestione dei segreti è seguire le indicazioni relative a rimozione, sostituzione e rotazione. Le credenziali più sicure sono quelle che non si devono memorizzare, gestire o trattare. Possono esserci credenziali non più necessarie per il funzionamento del carico di lavoro e che possono essere rimosse in modo sicuro.

Per le credenziali ancora necessarie per il corretto funzionamento del carico di lavoro, potrebbe esserci l'opportunità di sostituire le credenziali a lungo termine con credenziali temporanee o a breve termine. Ad esempio, invece di una codifica fissa di una chiave di accesso segreta AWS, si può pensare di sostituire le credenziali a lungo termine con credenziali temporanee utilizzando i ruoli IAM.

Alcuni segreti di lunga durata potrebbero non poter essere rimossi o sostituiti. È possibile archiviare tali segreti in un servizio come Gestione dei segreti AWS, dove saranno archiviati, gestiti e rotati a livello centrale su base regolare.

Un audit del codice sorgente e dei file di configurazione del carico di lavoro può rivelare molti tipi di credenziali. La tabella seguente riassume le strategie per gestire i tipi più comuni di credenziali:

Tipo di credenziali	Descrizione	Strategia suggerita
Chiavi di accesso IAM	Chiavi segrete e accesso IAM AWS utilizzate per assumere ruoli IAM all'interno di un carico di lavoro	Sostituzione: utilizza invece i ruoli IAM assegnati alle istanze di calcolo (come Amazon EC2 o AWS Lambda). Per l'interoperabilità con terze parti che richiedon o l'accesso alle risorse del tuo Account AWS, chiedi se supportano l'accesso multi-account AWS. Per le app mobili, prendi in considera zione l'utilizzo di credenziali

Tipo di credenziali	Descrizione	Strategia suggerita
		temporanee tramite pool di identità di Amazon Cognito (identità federate). Per i carichi di lavoro eseguiti all'esterno di AWS, valuta IAM Roles Anywhere o le attivazioni ibride di AWS Systems Manager. Per i container, consulta il ruolo IAM dell'attività di Amazon ECS o il ruolo IAM del nodo di Amazon ECS.
Chiavi SSH	Chiavi private Secure Shell utilizzate per accedere alle istanze Linux EC2, manualmente o nell'ambito di un processo automatizzato	Sostituzione: utilizza AWS Systems Manager o EC2 Instance Connect per fornire un accesso programmatico e umano alle istanze EC2 mediante i ruoli IAM.
Credenziali di applicazione e database	Password: stringa di testo semplice	Rotazione: memorizza le credenziali in Gestione dei segreti AWS e, laddove possibile, stabilisci una rotazione automatica.
Credenziali del database di amministrazione Aurora e Amazon RDS	Password: stringa di testo semplice	Sostituzione: utilizza l'integrazione di Secrets Manager con Amazon RDS o Amazon Aurora. Inoltre, alcuni tipi di database RDS possono utilizzare i ruoli IAM anziché le password per alcuni casi d'uso (per maggiori dettagli, consulta Autenticazione del database IAM).

Tipo di credenziali	Descrizione	Strategia suggerita
Token OAuth	Token segreti: stringa di testo semplice	Rotazione: archivia i token in Gestione dei segreti AWS e configura la rotazione automatica.
Token e chiavi API	Token segreti: stringa di testo semplice	Rotazione: archivia in Gestione dei segreti AWS e stabilisci una rotazione automatica, laddove possibile.

Un anti-pattern comune è quello di incorporare le chiavi di accesso IAM all'interno del codice sorgente, dei file di configurazione o delle applicazioni mobili. Se occorre una chiave di accesso IAM per la comunicazione con un servizio AWS, utilizza credenziali di sicurezza temporanee (a breve termine). È possibile fornire queste credenziali a breve termine tramite ruoli IAM per le istanze EC2, ruoli di esecuzione per le funzioni Lambda, ruoli IAM di Cognito per l'accesso degli utenti mobili e policy IoT Core per i dispositivi IoT. Nell'interfacciarsi con terze parti, è preferibile delegare l'accesso a un ruolo IAM con l'accesso necessario alle risorse dell'account anziché configurare un utente IAM e inviare alla terza parte la chiave di accesso segreta per l'utente interessato.

Esistono molti casi in cui il carico di lavoro richiede l'archiviazione dei segreti necessari per l'interoperabilità con altri servizi e risorse. Gestione dei segreti AWS è stato creato proprio per gestire in modo sicuro queste credenziali, nonché l'archiviazione, l'uso e la rotazione di token API, password e altre credenziali.

Gestione dei segreti AWS offre cinque funzionalità chiave per garantire la sicurezza di archiviazione e gestione delle credenziali sensibili: crittografia a riposo, crittografia in transito, audit completi, controllo granulare degli accessi e rotazione delle credenziali estensibile. Sono accettabili anche altri servizi di gestione dei segreti dei partner AWS o soluzioni sviluppate localmente che forniscano funzionalità e garanzie simili.

Quando si recupera un segreto, è possibile utilizzare il componente di caching lato client di Secrets Manager per memorizzarlo nella cache per un uso futuro. Il recupero di un segreto memorizzato nella cache è più veloce rispetto al recupero da Secrets Manager. Inoltre, poiché la chiamata alle API di Secrets Manager ha un costo, l'uso della cache può ridurre i costi. Per una descrizione di tutti i modi in cui è possibile recuperare i segreti, consulta Ottieni segreti.

> **Note**
>
> Alcune lingue possono richiedere l'implementazione di una propria crittografia in memoria per la cache lato client.

Passaggi dell'implementazione

1. Identifica i percorsi di codice con credenziali con codifica fissa mediante strumenti automatizzati come Amazon CodeGuru.
   a. Utilizza Amazon CodeGuru per eseguire la scansione dei repository di codice. Una volta completata l'analisi, filtra su Type=Secrets in CodeGuru per trovare righe di codice problematiche.
2. Identifica le credenziali che possono essere rimosse o sostituite.
   a. Identifica le credenziali non più necessarie e contrassegnarle per la rimozione.
   b. Le chiavi segrete AWS incorporate nel codice sorgente devono essere sostituite con ruoli IAM associati alle risorse necessarie. Se parte del tuo carico di lavoro è al di fuori di AWS ma richiede credenziali IAM per accedere a risorse AWS, prendi in considerazione IAM Roles Anywhere o le attivazioni ibride di AWS Systems Manager.
3. Per altri segreti di terze parti a lunga durata che richiedono l'uso della strategia di rotazione, integra Secrets Manager nel codice per recuperare i segreti di terze parti in fase di esecuzione.
   a. La console di CodeGuru può creare in automatico un segreto in Secrets Manager utilizzando le credenziali scoperte.
   b. Integra il recupero dei segreti da Secrets Manager nel codice dell'applicazione.
      i. Le funzioni Lambda serverless possono utilizzare un'estensione Lambda indipendente dal linguaggio.
      ii. Per container o istanze EC2, AWS fornisce un esempio di codice lato client per il recupero di segreti da Secrets Manager in diversi linguaggi di programmazione diffusi.
4. Esamina periodicamente la base di codice e ripetere la scansione per verificare che non siano stati aggiunti nuovi segreti al codice.
   a. Prendi in considerazione l'utilizzo di uno strumento come git-secrets per evitare di inserire nuovi segreti nel tuo repository di codice sorgente.
5. Monitora l'attività di Secrets Manager per individuare eventuali indicazioni di utilizzo imprevisto, accesso inopportuno ai segreti o tentativi di eliminazione degli stessi.

6. Riduci l'esposizione umana alle credenziali. Limita l'accesso alle credenziali di lettura, scrittura e modifica a un ruolo IAM dedicato a questo scopo e fornisci l'accesso in modo che il ruolo sia assunto solo da un piccolo sottoinsieme di utenti operativi.

Risorse

Best practice correlate:

- SEC02-BP02 Utilizzo di credenziali temporanee
- SEC02-BP05 Verifica e rotazione periodica delle credenziali

Documenti correlati:

- Nozioni di base su Gestione dei segreti AWS
- Identity Providers and Federation
- Amazon CodeGuru Introduces Secrets Detector
- How Gestione dei segreti AWS uses AWS Key Management Service
- Secret encryption and decryption in Secrets Manager
- Articoli del blog su Secrets Manager
- Amazon RDS announces integration with Gestione dei segreti AWS

Video correlati:

- Best Practices for Managing, Retrieving, and Rotating Secrets at Scale
- Find Hard-Coded Secrets Using Amazon CodeGuru Secrets Detector
- Securing Secrets for Hybrid Workloads Using Gestione dei segreti AWS

Workshop correlati:

- Store, retrieve, and manage sensitive credentials in Gestione dei segreti AWS
- AWS Systems Manager Hybrid Activations

SEC02-BP04 Fai affidamento su un gestore dell'identità digitale centralizzato

Per le identità della forza lavoro (dipendenti e collaboratori) affidati a un gestore dell'identità digitale che ti consenta di gestire le identità in un luogo centralizzato. In questo modo è più semplice gestire l'accesso tra più applicazioni e sistemi, poiché crei, assegni, gestisci, revochi e verifichi gli accessi da una singola posizione.

Risultato desiderato: hai un gestore dell'identità digitale dal quale gestisci centralmente gli utenti della forza lavoro, le policy di autenticazione (come le richieste di autenticazione a più fattori (MFA)) e le autorizzazioni per sistemi e applicazioni, come l'assegnazione dell'accesso in base all'appartenenza o agli attributi di un utente. Gli utenti che fanno parte della tua forza lavoro accedono al gestore dell'identità digitale centrale ed effettuano l'accesso federato (autenticazione unica) alle applicazioni interne ed esterne, il che elimina la necessità per gli utenti di ricordare più credenziali. Il gestore dell'identità digitale è integrato con i tuoi sistemi di risorse umane (HR), in modo che le modifiche relative al personale vengano sincronizzate in automatico con il gestore dell'identità digitale. Ad esempio, se qualcuno lascia l'organizzazione, puoi revocare automaticamente l'accesso alle applicazioni e ai sistemi federati (incluso AWS). Hai abilitato la verifica dettagliata dei log nel tuo gestore dell'identità digitale e stai monitorando questi log per rilevare comportamenti degli utenti insoliti.

Anti-pattern comuni:

- Non utilizzi federazione e autenticazione unica. Gli utenti che appartengono alla tua forza lavoro creano account utente e credenziali separati in più applicazioni e sistemi.
- Non hai automatizzato il ciclo di vita delle identità degli utenti che fanno parte della tua forza lavoro, ad esempio integrando il gestore dell'identità digitale con i tuoi sistemi HR. Quando un utente lascia l'organizzazione o cambia ruolo, segui una procedura manuale per eliminare o aggiornare i suoi record in più applicazioni e sistemi.

Vantaggi dell'adozione di questa best practice: utilizzare un gestore dell'identità digitale centralizzato ti fornisce un'unica piattaforma per gestire le identità e le policy degli utenti che fanno parte della tua forza lavoro, la possibilità di assegnare l'accesso alle applicazioni a utenti e gruppi e di monitorare l'attività di accesso degli utenti. Grazie all'integrazione con i sistemi di risorse umane (HR), quando un utente cambia ruolo, queste modifiche vengono sincronizzate con il gestore dell'identità digitale e le applicazioni e le autorizzazioni assegnate si aggiornano in automatico. Quando un utente lascia

l'organizzazione, la sua identità viene automaticamente disabilitata nel gestore dell'identità digitale e l'accesso alle applicazioni e ai sistemi federati viene revocato.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Guida per gli utenti della forza lavoro che accedono a AWS Gli utenti della forza lavoro, come i dipendenti e i collaboratori dell'organizzazione, possono richiedere l'accesso a AWS utilizzando la Console di gestione AWS o AWS Command Line Interface (AWS CLI) per svolgere le mansioni lavorative. Puoi concedere l'accesso ad AWS a tali utenti federando il tuo gestore dell'identità digitale centralizzato AWS a due livelli: federazione diretta a ciascun Account AWS o federazione a più account della tua organizzazione AWS.

Per federare gli utenti della tua forza lavoro direttamente con ciascun Account AWS, utilizza un gestore dell'identità digitale centralizzato per federare l'accesso ad AWS Identity and Access Management in tale account. Grazie alla sua flessibilità, IAM ti consente di abilitare un gestore dell'identità digitale SAML 2.0 o Open ID Connect (OIDC) separato per ciascun Account AWS e di utilizzare attributi per gli utenti federati al fine di controllare gli accessi. Gli utenti della tua forza lavoro utilizzano il proprio browser Web per accedere al gestore dell'identità digitale e forniscono le proprie credenziali (come password e codici token MFA). Il gestore dell'identità digitale rilascia un'asserzione SAML nel browser che viene inviata all'URL di accesso della Console di gestione AWS, così da consentire all'utente di accedere mediante l'autenticazione unica alla Console di gestione AWS assumendo un ruolo IAM. I tuoi utenti possono anche ottenere credenziali API AWS temporanee da AWS CLI o AWS SDK di AWS STS assumendo il ruolo IAM mediante un'asserzione SAML proveniente dal gestore dell'identità digitale.

Per federare gli utenti della forza lavoro con più account all'interno dell'organizzazione AWS, puoi usare Centro identità AWS IAM per gestire a livello centrale l'accesso degli utenti della forza lavoro agli Account AWS e alle applicazioni. Puoi abilitare il Centro identità per la tua organizzazione e configurare la tua origine di identità. Centro identità IAM fornisce una directory di origine di identità predefinita, utilizzabile per gestire utenti e gruppi. In alternativa, puoi scegliere un'origine di identità esterna connettendoti al tuo gestore dell'identità digitale esterno tramite SAML 2.0 e allocando in automatico utenti e gruppi tramite SCIM oppure connettendoti alla tua directory Microsoft AD mediante Directory Service. Una volta configurata un'origine di identità, puoi assegnare l'accesso agli Account AWS a utenti e gruppi, definendo policy di privilegio minimo nei tuoi set di autorizzazioni. Gli utenti della tua forza lavoro possono autenticarsi tramite il tuo gestore dell'identità digitale centrale per accedere al portale di accesso AWS ed eseguire l'accesso tramite autenticazione unica per gli Account AWS e le applicazioni cloud a loro assegnate. Gli utenti possono configurare AWS CLI

v2 per l'autenticazione con il Centro identità e ottenere le credenziali per eseguire i comandi AWS CLI. Il Centro identità consente inoltre l'accesso tramite SSO ad applicazioni AWS, come Amazon SageMaker Studio IA e i portali Sitewise AWS IoT.

Dopo aver seguito le indicazioni precedenti, gli utenti della forza lavoro non avranno più bisogno di utilizzare utenti IAM e gruppi per le normali operazioni quando gestiscono i carichi di lavoro su AWS. Gli utenti e i gruppi sono infatti gestiti all'esterno di AWS e sono in grado di accedere alle risorse AWS come identità federata. Le identità federate utilizzano i gruppi definiti dal gestore dell'identità digitale centralizzato. Devi identificare e rimuovere gruppi IAM, utenti IAM e credenziali utente di lunga durata (password e chiavi di accesso) non più necessarie nei tuoi Account AWS. Puoi trovare le credenziali inutilizzate mediante i report sulle credenziali IAM, eliminare gli utenti IAM corrispondenti ed eliminare i gruppi IAM. Puoi applicare una policy di controllo dei servizi alla tua organizzazione, così da prevenire la creazione di nuovi gruppi e utenti IAM, imponendo che l'accesso ad AWS avvenga tramite identità federate.

> **Note**
>
> L'utente è responsabile della gestione della rotazione dei token di accesso SCIM, come descritto nella documentazione sul provisioning automatico. Inoltre, l'utente è responsabile della rotazione dei certificati a supporto della federazione delle identità.

Guida per gli utenti delle applicazioni Puoi gestire le identità degli utenti delle applicazioni, ad esempio di un'applicazione per dispositivi mobili, utilizzando Amazon Cognito come gestore dell'identità digitale centralizzato. Amazon Cognito consente l'autenticazione, autorizzazione e gestione degli utenti per le app Web e per dispositivi mobili. Amazon Cognito offre un archivio di identità scalabile fino a milioni di utenti, supporta la federazione delle identità sociali e aziendali e offre funzionalità di sicurezza avanzate per proteggere i tuoi utenti e la tua azienda. Puoi integrare la tua applicazione Web o mobile personalizzata con Amazon Cognito per aggiungere l'autenticazione degli utenti e il controllo degli accessi alle applicazioni in pochi minuti. Amazon Cognito si fonda su standard di identità aperti come SAML e Open ID Connect (OIDC), supporta varie normative di conformità e si integra con le risorse di sviluppo frontend e backend.

Passaggi dell'implementazione

Passaggi per l'accesso ad AWS degli utenti della forza lavoro

- Federa l'accesso ad AWS degli utenti della tua forza lavoro tramite un gestore dell'identità digitale centralizzato seguendo uno dei seguenti approcci:

  - Utilizza il Centro identità IAM per abilitare l'accesso tramite autenticazione unica in più Account AWS nella tua organizzazione AWS con la federazione del tuo gestore dell'identità digitale.
  - Utilizza IAM per connettere il gestore dell'identità digitale direttamente a ciascun Account AWS, così da consentire un accesso federato e granulare.
- Identifica e rimuovi gruppi e utenti IAM sostituiti da identità federate.

Passaggi per gli utenti delle tue applicazioni

- Utilizza Amazon Cognito come gestore dell'identità digitale centralizzato per le tue applicazioni.
- Integra le tue applicazioni personalizzate con Amazon Cognito mediante OpenID Connect e OAuth. Puoi sviluppare applicazioni personalizzate utilizzando le librerie Amplify, che forniscono interfacce semplici da integrare con una varietà di servizi AWS per l'autenticazione, come Amazon Cognito.

Risorse

Best practice correlate:

- SEC02-BP06 Impiego dei gruppi di utenti e degli attributi
- SEC03-BP02 Concessione dell'accesso con privilegio minimo
- SEC03-BP06 Gestione degli accessi in base al ciclo di vita

Documenti correlati:

- Federazione delle identità in AWS
- Best practice per la sicurezza in IAM
- Best practice AWS Identity and Access Management
- Getting started with IAM Identity Center delegated administration
- How to use customer managed policies in IAM Identity Center for advanced use cases
- AWS CLI v2: provider di credenziali del Centro identità IAM

Video correlati:

- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) deep dive
- AWS re:Invent 2022 - Simplify your existing workforce access with IAM Identity Center

- AWS re:Invent 2018: Mastering Identity at Every Layer of the Cake

Esempi correlati:

- Workshop: Using AWS IAM Identity Center to achieve strong identity management

Strumenti correlati:

- AWS Security Competency Partner con competenze nella sicurezza: gestione di identità e accessi
- saml2aws

SEC02-BP05 Verifica e rotazione periodica delle credenziali

Sottoponi a audit e ruota periodicamente le credenziali per limitarne il tempo di utilizzo per l'accesso alle risorse. Le credenziali a lungo termine espongono a molti rischi, riducibili mediante la rotazione periodica.

Risultato desiderato: implementa la rotazione delle credenziali per ridurre i rischi associati all'utilizzo delle credenziali a lungo termine. Esegui regolarmente l'audit e rimedia alla non conformità con le policy di rotazione delle credenziali.

Anti-pattern comuni:

- Nessun audit dell'uso delle credenziali.
- Utilizzo non necessario di credenziali a lungo termine.
- Utilizzo di credenziali a lungo termine e mancata rotazione regolare.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Quando non è possibile fare affidamento sulle credenziali temporanee e occorrono credenziali a lungo termine, esegui l'audit delle credenziali per garantire l'applicazione dei controlli prestabiliti, ad esempio l'autenticazione a più fattori (MFA), la regolare rotazione e un livello di accesso appropriato.

La convalida periodica, preferibilmente tramite uno strumento automatizzato, è necessaria per verificare l'applicazione dei controlli corretti. Per le identità umane, è necessario richiedere agli utenti di modificare periodicamente le password e ritirare le chiavi di accesso a favore delle credenziali

temporanee. Nel passaggio dagli utenti AWS Identity and Access Management (IAM) alle identità centralizzate, puoi creare report sulle credenziali per controllare gli utenti.

Ti consigliamo inoltre di monitorare l'MFA nel tuo gestore dell'identità digitale. È possibile configurare Regole di AWS Config o utilizzare gli standard di sicurezza AWS Security Hub CSPM per monitorare se gli utenti hanno configurato l'MFA. Valuta la possibilità di utilizzare IAM Roles Anywhere per fornire credenziali temporanee per le identità macchina. Nelle situazioni in cui l'utilizzo di credenziali temporanee e ruoli IAM non è possibile, sono necessari audit e rotazione frequenti delle chiavi di accesso.

Passaggi dell'implementazione

- Esegui con regolarità audit delle credenziali: l'audit delle identità configurate nel tuo gestore dell'identità digitale e in IAM consente di verificare che l'accesso al tuo carico di lavoro sia concesso solo alle identità autorizzate. Tali identità possono includere, a titolo esemplificativo ma non esaustivo, utenti IAM, utenti del Centro identità AWS IAM, utenti di Active Directory o utenti di altri gestori dell'identità digitale upstream. Ad esempio, eliminare le persone che lasciano l'organizzazione e i ruoli multi-account non più necessari. Predisponi un processo per sottoporre periodicamente ad audit le autorizzazioni ai servizi a cui accede un'entità IAM. In questo modo potrai identificare le policy da modificare per rimuovere le autorizzazioni non utilizzate. Utilizza i report delle credenziali e AWS Identity and Access Management Access Analyzer per eseguire l'audit di credenziali e autorizzazioni IAM. Usa Amazon CloudWatch per configurare allarmi per chiamate API specifiche chiamate all'interno del tuo ambiente AWS. Amazon GuardDuty può inoltre avvisarti in caso attività impreviste, possibili segnali di un accesso eccessivamente permissivo o un accesso non intenzionale alle credenziali IAM.
- Ruota le credenziali regolarmente: se non puoi utilizzare credenziali temporanee, ruota con regolarità le chiavi di accesso IAM a lungo termine (massimo ogni 90 giorni). In caso di divulgazione involontaria e a propria insaputa di una chiave di accesso, questo limita la durata di utilizzo delle credenziali per accedere alle risorse. Per informazioni sulla rotazione delle chiavi di accesso per gli utenti IAM, consulta Rotazione delle chiavi di accesso.
- Rivedi le autorizzazioni IAM: per migliorare la sicurezza del tuo Account AWS, rivedi con regolarità e monitora ciascuna policy IAM. Verifica che le policy rispettino il principio del privilegio minimo.
- Valuta la possibilità di automatizzare la creazione e gli aggiornamenti delle risorse IAM: il Centro identità IAM automatizza molte attività IAM, come la gestione di ruoli e policy. In alternativa, AWS CloudFormation può essere utilizzato per automatizzare l'implementazione delle risorse IAM, compresi ruoli e policy, per ridurre la possibilità di errore umano, poiché i modelli possono essere verificati e controllati in versione.

- Usa IAM Roles Anywhere per sostituire gli utenti IAM per le identità macchina: IAM Roles Anywhere consente di utilizzare i ruoli in aree in cui prima non era possibile, come i server on-premises. IAM Roles Anywhere utilizza un certificato X.509 attendibile per l'autenticazione a AWS e la ricezione di credenziali temporanee. L'utilizzo di IAM Roles Anywhere evita la necessità di ruotare queste credenziali, poiché le credenziali a lungo termine non vengono più memorizzate nell'ambiente on-premises. È necessario monitorare e ruotare il certificato X.509 quando si avvicina alla scadenza.

Risorse

Best practice correlate:

- SEC02-BP02 Utilizzo di credenziali temporanee
- SEC02-BP03 Archiviazione e utilizzo dei segreti in modo sicuro

Documenti correlati:

- Nozioni di base su Gestione dei segreti AWS
- Best practice di IAM
- Identity Providers and Federation
- Soluzioni dei partner per la sicurezza: accesso e controllo degli accessi
- Temporary Security Credentials
- Recupero dei report delle credenziali per l'Account AWS

Video correlati:

- Best Practices for Managing, Retrieving, and Rotating Secrets at Scale
- Managing user permissions at scale with AWS IAM Identity Center
- Mastering identity at every layer of the cake

SEC02-BP06 Impiego dei gruppi di utenti e degli attributi

Definire le autorizzazioni in base a gruppi di utenti e attributi aiuta a ridurre numero e complessità delle policy, semplificando il raggiungimento del principio del privilegio minimo. Puoi usare i gruppi

di utenti per gestire le autorizzazioni di molte persone in un'unica posizione, in base alla funzione svolte nell'organizzazione. Gli attributi, come il reparto, il progetto o la posizione, possono fornire un ulteriore livello di portata dei permessi quando le persone svolgono una funzione simile ma per sottoinsiemi diversi di risorse.

Risultato desiderato: puoi applicare modifiche alle autorizzazioni in base alla funzione per tutti gli utenti che la eseguono. L'appartenenza al gruppo e gli attributi regolano le autorizzazioni degli utenti, riducendo la necessità di gestire le autorizzazioni a livello di singolo utente. I gruppi e gli attributi definiti nel gestore dell'identità digitale vengono propagati automaticamente agli ambienti AWS.

Anti-pattern comuni:

- Gestione delle autorizzazioni per singoli utenti e duplicazione tra più utenti.
- Definizione dei gruppi a un livello troppo alto, concessione di autorizzazioni troppo estese.
- Definizione di gruppi a un livello troppo granulare, che crea duplicazioni e confusione sull'appartenenza.
- Utilizzo di gruppi con autorizzazioni duplicate su sottoinsiemi di risorse quando è possibile utilizzare invece gli attributi.
- Nessuna gestione di gruppi, attributi e appartenenze attraverso un gestore dell'identità digitale standardizzato e integrato con gli ambienti AWS.
- Utilizzo della concatenazione dei ruoli quando si utilizzano le sessioni di Centro identità AWS IAM

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

Le autorizzazioni AWS sono definite nei documenti denominati policy, associati a un principale, ad esempio un utente, gruppo, ruolo o risorsa. Puoi scalare la gestione delle autorizzazioni organizzando le assegnazioni delle autorizzazioni (gruppo, autorizzazioni, account) in base alla funzione lavorativa, al carico di lavoro e all'ambiente SDLC. Per la forza lavoro, ciò consente di definire i gruppi in base alla funzione svolta dagli utenti per l'organizzazione, anziché in base alle risorse a cui si accede. Ad esempio, un gruppo WebAppDeveloper può avere una policy collegata per la configurazione di servizi come Amazon CloudFront all'interno di un account di sviluppo. Un gruppo `AutomationDeveloper` può avere alcune autorizzazioni che si sovrappongono a quelle del gruppo `WebAppDeveloper`. Queste autorizzazioni comuni possono essere acquisite in una policy separata e associate a entrambi i gruppi, anziché avere utenti di entrambe le funzioni che appartengono a un gruppo `CloudFrontAccess`.

Oltre ai gruppi, è possibile utilizzare gli attributi per un ulteriore ambito dell'accesso. Ad esempio, è possibile avere un attributo Project per gli utenti del gruppo `WebAppDeveloper`, per limitare l'accesso alle risorse specifiche del loro progetto. L'uso di questa tecnica elimina la necessità di avere gruppi diversi per gli sviluppatori di applicazioni che lavorano su progetti diversi, se le loro autorizzazioni sono comunque le stesse. Il modo in cui si fa riferimento agli attributi nelle policy di autorizzazione si basa sulla loro origine, indipendentemente dal fatto che siano definiti come parte del protocollo di federazione (come SAML, OIDC o SCIM), come asserzioni SAML personalizzate o impostati all'interno del Centro identità IAM.

Passaggi dell'implementazione

1. Stabilisci dove definire gruppi e attributi:
   a. Seguendo le indicazioni riportate in SEC02-BP04 Fai affidamento su un gestore dell'identità digitale centralizzato, puoi determinare se occorre definire gruppi e attributi all'interno del gestore dell'identità digitale, all'interno del Centro identità IAM o utilizzare i gruppi di utenti IAM in un account specifico.
2. Definisci i gruppi:
   a. Determina i tuoi gruppi in base alla funzione e all'ambito di accesso richiesti. Valuta se utilizzare una struttura gerarchica o di convenzioni di denominazione per organizzare i gruppi in modo efficace.
   b. Se procedi alla definizione all'interno del Centro identità IAM, crea i gruppi e associa il livello di accesso desiderato utilizzando i set di autorizzazioni.
   c. Se definisci all'interno di un gestore dell'identità digitale esterno, determina se il gestore supporta il protocollo SCIM e valuta la possibilità di abilitare il provisioning automatico all'interno del Centro identità IAM. Questa funzionalità sincronizza la creazione, l'appartenenza e l'eliminazione di gruppi tra il tuo gestore e il Centro identità IAM.
3. Definisci gli attributi:
   a. Se utilizzi un gestore dell'identità digitale esterno, entrambi i protocolli SCIM e SAML 2.0 forniscono determinati attributi per impostazione predefinita. È possibile definire attributi aggiuntivi e trasferirli mediante le asserzioni SAML con il nome dell'attributo `https://aws.amazon.com/SAML/Attributes/PrincipalTag`. Consulta la documentazione del gestore dell'identità digitale per le istruzioni sulla definizione e la configurazione di attributi personalizzati.
   b. Se definisci i ruoli all'interno di Centro identità IAM, abilita la funzionalità di controllo degli accessi basato su attributi (ABAC) e definisci gli attributi come desiderato. Considera gli attributi che si allineano alla struttura dell'organizzazione o alla strategia di tagging delle risorse.

Se richiedi il concatenamento dei ruoli IAM da ruoli IAM assunti tramite Centro identità IAM, i valori come `source-identity` e `principal-tags` non si propagano. Per ulteriori dettagli, consulta Enable and configure attributes for access control.

1. Autorizzazioni di ambito basate su gruppi e attributi:
    a. Prendi in considerazione la possibilità di includere nelle tue policy di autorizzazione condizioni che confrontino gli attributi del tuo principale con gli attributi delle risorse a cui si accede. Ad esempio, puoi definire una condizione che consenta l'accesso a una risorsa solo se il valore di una chiave di condizione `PrincipalTag` corrisponde a quello di una chiave `ResourceTag` con lo stesso nome.
    b. Per la definizione delle policy ABAC, segui le indicazioni contenute nelle best practice e negli esempi relativi alle autorizzazioni ABAC.
    c. Rivedi e aggiorna regolarmente la struttura dei gruppi e degli attributi in base all'evoluzione delle esigenze dell'organizzazione per garantire una gestione ottimale delle autorizzazioni.

Risorse

Best practice correlate:

- SEC02-BP04 Fai affidamento su un gestore dell'identità digitale centralizzato
- SEC03-BP02 Concessione dell'accesso con privilegio minimo
- COST02-BP04 Implementazione di gruppi e ruoli

Documenti correlati:

- Best practice di IAM
- Manage Identities in IAM Identity Center
- What Is ABAC for AWS?
- ABAC In IAM Identity Center
- ABAC Policy Examples

Video correlati:

- Managing user permissions at scale with AWS IAM Identity Center
- Mastering identity at every layer of the cake

Gestione delle autorizzazioni

Gestisci le autorizzazioni per controllare l'accesso alle identità di persone e macchine che richiedono l'accesso ad AWS e ai tuoi carichi di lavoro. Le autorizzazioni consentono di controllare chi può accedere a cosa e a quali condizioni. Impostando le autorizzazioni per specifiche identità umane e di macchine, si concede loro l'accesso a determinate azioni di servizio su risorse specifiche. Inoltre, è possibile specificare le condizioni che devono essere vere per concedere l'accesso.

Esistono modi diversi per concedere l'accesso a diversi tipi di risorse. Un modo è tramite l'uso di diversi tipi di policy.

Le policy basate sull'identità in IAM sono gestite o in linea e si collegano alle identità IAM, il che comprende utenti, gruppi o ruoli. Queste policy consentono di specificare cosa può fare quell'identità (le sue autorizzazioni). Le policy basate sulle identità possono essere ulteriormente categorizzate.

Policy gestite: le policy autonome basate sulle identità che possono essere collegate a più utenti, gruppi o ruoli nell'account AWS. Sono disponibili due tipi di policy gestite.

- Policy gestite da AWS: le policy gestite che sono create e gestite da AWS.
- Policy gestite dal cliente: le policy gestite che sono create e gestite nell'account AWS. Le policy gestite dal cliente offrono un controllo maggiore sulle policy rispetto alle policy gestite da AWS.

Le policy gestite sono il metodo migliore per applicare le autorizzazioni. Tuttavia, puoi anche usare policy inline che aggiungi direttamente a un singolo utente, gruppo o ruolo. Le policy inline sono utili per mantenere una stretta relazione uno a uno tra una policy e un'identità. Le policy inline vengono eliminate quando elimini l'identità.

Nella maggior parte dei casi, devi creare policy gestite dal cliente proprietarie seguendo il principio del privilegio minimo.

Le policy basate su risorse sono collegate a una risorsa. Ad esempio, una policy del bucket S3 è una policy basata su risorse. Queste policy concedono l'autorizzazione a un principale che può essere nello stesso account della risorsa o in un altro account. Per un elenco dei servizi che supportano le policy basate sulle risorse, consulta Servizi AWS che funzionano con IAM.

I limiti delle autorizzazioni usano una policy gestita per impostare il numero massimo di autorizzazioni che un amministratore può impostare. In questo modo puoi delegare la possibilità di creare e gestire le autorizzazioni agli sviluppatori, ad esempio la creazione di un ruolo IAM, ma limitare le

autorizzazioni che possono concedere in modo che non possano inoltrare l'autorizzazione utilizzando ciò che hanno creato.

Il controllo degli accessi basato su attributi (ABAC) in AWS consente di concedere autorizzazioni in base agli attributi, che sono detti tag. I tag possono essere collegati alle entità principali IAM (utenti o ruoli) e alle risorse AWS. Gli amministratori possono creare policy IAM riutilizzabili che applicano le autorizzazioni in base agli attributi dell'entità principale IAM. Ad esempio, in qualità di amministratore puoi utilizzare una singola policy IAM che concede agli sviluppatori dell'organizzazione l'accesso alle risorse AWS che corrispondono ai tag di progetto. Man mano che il team di sviluppatori aggiunge risorse ai progetti, le autorizzazioni vengono applicate automaticamente in base agli attributi, eliminando la necessità di aggiornare le policy per ogni nuova risorsa.

Le policy di controllo dei servizi delle organizzazioni definiscono il numero massimo di autorizzazioni per i membri dell'account di un'organizzazione o un'unità organizzativa (UO). Le SCP limitano le autorizzazioni che le policy basate su identità o le policy basate su risorse concedono alle entità (utenti o ruoli) all'interno dell'account, ma non concedono autorizzazioni.

Le policy di sessione presuppongono un ruolo o un utente federato. Migra le policy di sessione quando usi AWS CLI o AWS API Le policy di sessione limitano le autorizzazioni che le policy del ruolo o dell'utente basate su identità concedono alla sessione. Le policy di sessione limitano le autorizzazioni per una sessione creata, ma non concedono autorizzazioni. Per ulteriori informazioni, consulta la sezione relativa alle policy di sessione.

Best practice

- SEC03-BP01 Definizione dei requisiti di accesso
- SEC03-BP02 Concessione dell'accesso con privilegio minimo
- SEC03-BP03 Determinazione di un processo per l'accesso di emergenza
- SEC03-BP04 Riduzione delle autorizzazioni in modo continuo
- SEC03-BP05 Definizione dei guardrail per le autorizzazioni dell'organizzazione
- SEC03-BP06 Gestione degli accessi in base al ciclo di vita
- SEC03-BP07 Analisi dell’accesso multi-account e pubblico
- SEC03-BP08 Condivisione delle risorse in modo sicuro all'interno dell'organizzazione
- SEC03-BP09 Condivisione sicura delle risorse con terze parti

SEC03-BP01 Definizione dei requisiti di accesso

Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autenticazione e autorizzazione appropriati.

Anti-pattern comuni:

- Codifica fissa o archiviazione dei segreti nell'applicazione.
- Concessione di autorizzazioni personalizzate per ogni utente.
- Utilizzo di credenziali di lunga durata.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autenticazione e autorizzazione appropriati.

L'accesso regolare agli Account AWS all'interno di un'organizzazione dovrebbe essere fornito utilizzando l'accesso federato o un gestore dell'identità digitale centralizzato. Occorre anche centralizzare la gestione delle identità e garantire la presenza di una procedura consolidata per integrare l'accesso ad AWS nel ciclo di vita dell'accesso dei dipendenti. Ad esempio, se un dipendente passa a un ruolo lavorativo con un livello di accesso diverso, anche la sua appartenenza al gruppo deve cambiare per riflettere i nuovi requisiti di accesso.

Nel definire i requisiti di accesso per le identità non umane, determina quali applicazioni e componenti devono accedere, nonché le modalità di concessione delle autorizzazioni. L'utilizzo di ruoli IAM creati con il modello di accesso con privilegio minimo è un approccio consigliato. AWS Le policy gestite forniscono le policy IAM predefinite che coprono la maggior parte dei casi d'uso comuni.

I servizi AWS, come Gestione dei segreti AWS e l'archivio dei parametri AWS Systems Manager consentono di separare i segreti dall'applicazione o dal carico di lavoro in modo sicuro. In Secrets Manager, puoi adottare la rotazione automatica delle credenziali. Puoi usare Systems Manager per fare riferimento a parametri negli script, comandi, documenti SSM, configurazione e flussi di lavoro di automazione utilizzando il nome univoco specificato al momento della creazione del parametro.

Puoi utilizzare AWS IAM Roles Anywhere per ottenere credenziali di sicurezza temporanee in IAM per carichi di lavoro eseguiti all'esterno di AWS. I tuoi carichi di lavoro possono utilizzare le stesse policy IAM e gli stessi ruoli IAM che utilizzi con le applicazioni AWS per accedere alle risorse AWS.

Ove possibile, prediligi le credenziali temporanee a breve termine rispetto a quelle statiche a lungo termine. Per gli scenari in cui occorrono utenti con accesso programmatico e credenziali a lungo termine, usa le ultime informazioni usate per la chiave di accesso per la rotazione e la rimozione delle chiavi di accesso.

Gli utenti hanno bisogno di un accesso programmatico se desiderano interagire con AWS esternamente a Console di gestione AWS. La modalità con cui concedere l'accesso programmatico dipende dal tipo di utente che accede ad AWS.

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
IAM	(Consigliato) Utilizza credenziali della console come credenziali temporanee per firmare richieste programmatiche alla AWS CLI, agli SDK AWS o alle API AWS.	Segui le istruzioni per l'interfaccia che desideri utilizzare. • Per AWS CLI, consulta Accesso allo sviluppo locale di AWS nella Guida per l'utente di AWS Command Line Interface. • Per gli SDK AWS, consulta Accesso per lo sviluppo AWS locale nella Guida di riferimento agli SDK e agli strumenti AWS.
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporanee per firmare richieste programmatiche alla AWS CLI, agli SDK AWS o alle API AWS.	Segui le istruzioni per l'interfaccia che desideri utilizzare. • Per la AWS CLI, consulta la pagina Configurazione della AWS CLI per l'uso di AWS

Quale utente necessita dell'accesso programmatico?	Per	Come
		IAM Identity Center nella Guida per l'utente dell'AWS Command Line Interface. • Per gli SDK AWS, gli strumenti e le API AWS, consulta la pagina Autenticazione Centro identità IAM nella Guida di riferimento per SDK e strumenti AWS.
IAM	Utilizza credenziali temporane e per firmare richieste programmatiche alla AWS CLI, agli SDK AWS o alle API AWS.	Segui le istruzioni in Utilizzo di credenziali temporanee con le risorse AWS nella Guida per l'utente IAM.

Quale utente necessita dell'accesso programmatico?	Per	Come
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare richieste programmatiche alla AWS CLI, agli SDK AWS o alle API AWS.	Segui le istruzioni per l'interfaccia che desideri utilizzare. • Per la AWS CLI, consulta la pagina Autenticazione tramite credenziali utente IAM nella Guida per l'utente dell'AWS Command Line Interface. • Per gli SDK e gli strumenti AWS, consulta la pagina Autenticazione con credenziali a lungo termine nella Guida di riferimento per SDK e strumenti AWS. • Per le API AWS, consulta la pagina Gestione delle chiavi di accesso per utenti IAM nella Guida per l'utente IAM.

Risorse

Documenti correlati:

- Controllo degli accessi basato su attributi (ABAC)
- AWS IAM Identity Center
- IAM Roles Anywhere di
- AWS Managed policies for IAM Identity Center
- AWS Condizioni delle policy IAM
- Casi d'uso IAM
- Rimuovere credenziali non necessarie
- Lavorare con le policy

- How to control access to AWS resources based on Account AWS, OU, or organization
- Identify, arrange, and manage secrets easily using enhanced search in Gestione dei segreti AWS

Video correlati:

- Become an IAM Policy Master in 60 Minutes or Less
- Separation of Duties, Least Privilege, Delegation, and CI/CD
- Streamlining identity and access management for innovation

SEC03-BP02 Concessione dell'accesso con privilegio minimo

Concedi solo l'accesso richiesto dagli utenti per eseguire azioni specifiche su determinate risorse in condizioni particolari. Affidati a gruppi e attributi di identità per impostare in modo dinamico le autorizzazioni su vasta scala, anziché definire le autorizzazioni per i singoli utenti. Ad esempio, puoi concedere a un gruppo di sviluppatori le autorizzazioni per gestire solo le risorse del loro progetto. In questo modo, se uno sviluppatore lascia il progetto, l'accesso viene revocato in automatico senza modificare le policy di accesso sottostanti.

Risultato desiderato: gli utenti dispongono solo delle autorizzazioni minime richieste per le funzioni lavorative specifiche. Utilizzi Account AWS separati per isolare gli sviluppatori dagli ambienti di produzione. Quando gli sviluppatori devono accedere agli ambienti di produzione per attività specifiche, viene concesso un accesso limitato e controllato solo per la durata di tali attività. L'accesso alla produzione viene immediatamente revocato al termine del lavoro necessario. Esegui revisioni regolari delle autorizzazioni e revocale prontamente quando non sono più necessarie, ad esempio quando un utente cambia ruolo o lascia l'organizzazione. Limita i privilegi di amministratore a un gruppo ristretto e attendibile per ridurre l'esposizione al rischio. Assegna agli account di computer o di sistema solo le autorizzazioni minime necessarie per eseguire le attività previste.

Anti-pattern comuni:

- Per impostazione predefinita, concedi agli utenti le autorizzazioni di amministratore.
- Utilizzi l'account utente root per le attività quotidiane.
- Crei policy eccessivamente permissive senza un ambito adeguato.
- Le revisioni delle autorizzazioni sono rare, il che porta all'insinuarsi di autorizzazioni.
- Per l'isolamento dell'ambiente o la gestione delle autorizzazioni, fai affidamento esclusivamente al controllo degli accessi basato su attributi.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Secondo il principio del privilegio minimo, le identità dovrebbero essere autorizzate a eseguire solo il più piccolo insieme di azioni necessarie per lo svolgimento di un'attività specifica. In questo modo usabilità, efficienza e sicurezza sono bilanciate. Seguendo questo principio si limitano gli accessi indesiderati e si può monitorare chi accede a quali risorse. Per impostazione predefinita, ruoli e utenti IAM non dispongono di autorizzazioni. Per impostazione predefinita, l'utente root dispone dell'accesso completo e deve essere strettamente controllato, monitorato e utilizzato solo per le attività che richiedono l'accesso root.

Le policy IAM consentono di concedere in modo esplicito le autorizzazioni ai ruoli IAM o a risorse specifiche. Ad esempio, le policy basate su identità possono essere collegate ai gruppi IAM, mentre i bucket S3 possono essere controllati da policy basate su risorse.

Quando crei una policy IAM, puoi specificare le azioni di servizio, le risorse e le condizioni che devono essere vere affinché AWS consenta o rifiuti l'accesso. AWS supporta una serie di condizioni per aiutare a ridurre l'ambito dell'accesso. Ad esempio, con la chiave di condizione PrincipalOrgID, puoi negare azioni se il richiedente non fa parte della tua organizzazione AWS.

Puoi anche controllare le richieste effettuate dai servizi AWS per tuo conto, ad esempio AWS CloudFormation per la creazione di una funzione AWS Lambda, utilizzando la chiave di condizione CalledVia. Puoi stratificare diversi tipi di policy per stabilire una difesa in profondità e limitare le autorizzazioni complessive degli utenti. Puoi anche limitare le autorizzazioni che possono essere concesse e le relative condizioni. Ad esempio, puoi consentire ai team del carico di lavoro di creare le proprie policy IAM per i sistemi che realizzano, ma solo se applicano un limite delle autorizzazioni per circoscrivere le autorizzazioni massime che possono essere concesse.

Passaggi dell'implementazione

- Implementa policy con privilegio minimo: assegna policy di accesso con privilegio minimo a ruoli e gruppi IAM in modo da rispecchiare il ruolo o la funzione dell'utente che hai definito.
- Isola gli ambienti di sviluppo e produzione tramite Account AWS separati: utilizza Account AWS separati per gli ambienti di sviluppo e di produzione e controlla l'accesso tra di essi utilizzando policy di controllo dei servizi, policy delle risorse e policy identità.
- Policy di base sull'utilizzo delle API: un modo per determinare le autorizzazioni necessarie consiste nel rivedere i log AWS CloudTrail. Puoi utilizzare questa revisione per creare autorizzazioni personalizzate in base alle azioni che l'utente esegue effettivamente all'interno di AWS. IAM

Access Analyzer può generare automaticamente una policy IAM basata su attività di accesso. Puoi usare IAM Access Advisor a livello di organizzazione o account per tenere traccia delle ultime informazioni a cui si ha avuto accesso per una particolare policy.

- Prendi in considerazione l'utilizzo di policy gestite da AWS per funzioni lavorative: quando inizi a creare policy di autorizzazioni granulari, può essere utile utilizzare policy gestite da AWS per ruoli lavorativi comuni, ad esempio contabili, amministratori di database e data scientist. Questi policy possono aiutare a restringere l'accesso degli utenti mentre si determina come implementare i criteri di privilegio minimo.
- Rimuovi le autorizzazioni non necessarie: rileva e rimuovi le entità, le credenziali e le autorizzazioni IAM non utilizzate per ottenere il principio del privilegio minimo. Puoi utilizzare Sistema di analisi degli accessi AWS IAM per identificare gli accessi esterni e quelli non utilizzati e la generazione di policy del Sistema di analisi degli accessi AWS IAM può aiutare a eseguire il fine-tuning delle policy di autorizzazione.
- Assicurati che gli utenti abbiano un accesso limitato agli ambienti di produzione: gli utenti devono avere accesso agli ambienti di produzione solo in presenza di un caso d'uso valido. Una volta eseguite le attività specifiche che richiedono l'accesso alla produzione, l'accesso dell'utente deve essere revocato. Limitare l'accesso agli ambienti di produzione contribuisce a evitare eventi indesiderati con impatto sulla produzione e contiene gli effetti di accessi involontari.
- Considera i confini delle autorizzazioni: un limite delle autorizzazioni è una funzionalità per l'utilizzo di una policy gestita che stabilisce le autorizzazioni massime che una policy basata sull'identità può concedere a un'entità IAM. Il limite delle autorizzazioni di un'entità consente di eseguire solo le operazioni consentite dalle sue policy basate su identità e dai suoi limiti delle autorizzazioni.
- Perfeziona l'accesso usando il controllo dell'accesso basato sugli attributi e i tag delle risorse Il controllo degli accessi basato su attributi (ABAC) usando i tag delle risorse può essere usato per perfezionare le autorizzazioni quando è supportato. Puoi utilizzare un modello ABAC che confronta i tag dei principali con i tag delle risorse per perfezionare l'accesso in base a dimensioni personalizzate definite dall'utente. Questo approccio può semplificare e ridurre il numero di policy di autorizzazione nell'organizzazione.
  - Si consiglia di utilizzare ABAC per il controllo degli accessi solo quando sia i principali che le risorse sono di proprietà dell'organizzazione AWS. Le parti esterne possono utilizzare gli stessi nomi e valori di tag dell'organizzazione per i propri principali e risorse. Se fai affidamento esclusivamente su queste coppie nome-valore per concedere l'accesso a risorse o principali esterni, potresti fornire autorizzazioni indesiderate.
- Utilizza le policy di controllo dei servizi per AWS Organizations: le policy di controllo dei servizi controllano centralmente le autorizzazioni massime disponibili per gli account dei membri

dell'organizzazione. È importante notare che puoi utilizzare le policy di controllo dei servizi per limitare le autorizzazioni dell'utente root negli account membri. Prendi anche in considerazione la possibilità di usare AWS Control Tower, che offre controlli gestiti prescrittivi che arricchiscono AWS Organizations. Puoi anche definire i tuoi controlli in Control Tower.

- Stabilisci una policy del ciclo di vita degli utenti per la tua organizzazione: le policy del ciclo di vita degli utenti definiscono le attività da eseguire in caso di onboarding degli utenti in AWS, cambiamento di ruolo o ambito lavorativo o cessata necessità di accedere a AWS. Esegui revisioni delle autorizzazioni durante ogni fase del ciclo di vita di un utente per verificare che le autorizzazioni siano adeguatamente restrittive e per evitare l'insorgere di autorizzazioni.
- Stabilisci una pianificazione regolare per rivedere le autorizzazioni e rimuovere quelle non necessarie: è necessario rivedere regolarmente l'accesso utente per verificare che non sia eccessivamente permissivo. AWS Config e Sistema di analisi degli accessi AWS IAM possono essere d'aiuto durante gli audit delle autorizzazioni degli utenti.
- Stabilisci una matrice dei ruoli professionali: una matrice dei ruoli professionali visualizza i vari ruoli e i livelli di accesso richiesti all'interno della tua impronta AWS. Con una matrice dei ruoli professionali puoi definire e separare le autorizzazioni in base alle responsabilità degli utenti all'interno dell'organizzazione. Utilizza i gruppi anziché applicare le autorizzazioni direttamente a singoli utenti o ruoli.

Risorse

Documenti correlati:

- Grant least privilege
- Permissions boundaries for IAM entities
- Techniques for writing least privilege IAM policies
- IAM Access Analyzer makes it easier to implement least privilege permissions by generating IAM policies based on access activity
- Delegate permission management to developers by using IAM permissions boundaries
- Perfezionare le autorizzazioni utilizzando le informazioni dell'ultimo accesso
- IAM policy and when to use them
- Test delle policy IAM con il simulatore di policy IAM
- Guardrail in AWS Control Tower
- Zero Trust architectures: An AWS perspective

- How to implement the principle of least privilege with CloudFormation StackSets
- Controllo degli accessi basato su attributi (ABAC)
- Reducing policy scope by viewing user activity
- View role access
- Uso dei tag per organizzare il proprio ambiente e aumentare la responsabilità
- Strategie di applicazione di tag AWS
- Applicazione di tag alle risorse AWS

Video correlati:

- Next-generation permissions management
- Zero Trust: An AWS perspective

SEC03-BP03 Determinazione di un processo per l'accesso di emergenza

Crea un processo che consenta l'accesso di emergenza ai tuoi carichi di lavoro nell'improbabile eventualità che si verifichi un problema con il tuo gestore dell'identità digitale centralizzato.

Devi progettare processi per diverse modalità di guasto che potrebbero causare un evento di emergenza. Ad esempio, in circostanze normali, gli utenti della tua forza lavoro si federano nel cloud utilizzando un gestore dell'identità digitale centralizzato (SEC02-BP04) per gestire i loro carichi di lavoro. Tuttavia, se il tuo gestore dell'identità digitale centralizzato riscontra un errore o la configurazione per la federazione nel cloud subisce modifiche, gli utenti della tua forza lavoro potrebbero non essere in grado di federarsi nel cloud. Un processo di accesso di emergenza consente agli amministratori autorizzati di accedere alle risorse cloud tramite mezzi alternativi (come una forma alternativa di federazione o l'accesso diretto degli utenti) per risolvere problemi relativi alla configurazione della federazione o ai carichi di lavoro. Si ricorre al processo di accesso di emergenza fino al ripristino del normale meccanismo di federazione.

Risultato desiderato:

- Hai definito e documentato le modalità di guasto che costituiscono un'emergenza: considera le circostanze normali e i sistemi da cui dipendono gli utenti per gestire i loro carichi di lavoro. Prendi in considerazione quali guasti possono interessare ciascuna di queste dipendenze e causare una situazione di emergenza. Potresti trovare utili le domande e le best practice del pilastro

dell'affidabilità per individuare le modalità di errore e progettare sistemi più resilienti al fine di ridurre al minimo la probabilità di guasti.

- Hai documentato i passaggi da seguire per confermare che un guasto costituisce un'emergenza. Ad esempio, puoi richiedere agli amministratori di identità di controllare lo stato dei gestori delle identità digitali primari e di standby e, se entrambi non sono disponibili, dichiarare un evento di emergenza per guasto del gestore dell'identità digitale.
- È stato definito un processo di accesso di emergenza specifico per ogni tipo di modalità di emergenza o di guasto. Essere specifici può ridurre la tentazione da parte degli utenti di abusare di un processo generale per tutti i tipi di emergenze. I processi di accesso di emergenza illustrano le circostanze in cui ciascun processo va o non va utilizzato e indicano processi alternativi applicabili.
- I tuoi processi sono ben documentati con istruzioni e playbook dettagliati, facili da mettere in pratica in modo rapido ed efficiente. Ricorda che un evento di emergenza può essere un momento stressante per i tuoi utenti, che potrebbero essere sotto pressione per motivi di tempo, quindi progetta il tuo processo in modo che sia il più semplice possibile.

Anti-pattern comuni:

- Non si dispone di procedure di accesso di emergenza ben documentate e collaudate. Gli utenti non sono preparati per un'emergenza e seguono processi improvvisati quando si verifica un evento di emergenza.
- I processi di accesso di emergenza dipendono dagli stessi sistemi (come un gestore dell'identità digitale centralizzato) dei normali meccanismi di accesso. Ciò significa che il guasto di un sistema di questo tipo può influire sui normali meccanismi di accesso e di emergenza e compromettere la capacità di ripristino dall'errore.
- I processi di accesso di emergenza vengono utilizzati in situazioni non di emergenza. Ad esempio, gli utenti utilizzano spesso in modo improprio i processi di accesso di emergenza poiché trovano più facile apportare modifiche direttamente piuttosto che inviarle tramite una pipeline.
- I processi di accesso di emergenza non generano log sufficienti per effettuare l'audit dei processi oppure i log non vengono monitorati per segnalare un potenziale uso improprio dei processi.

Vantaggi dell'adozione di questa best practice:

- Grazie a processi di accesso di emergenza ben documentati e collaudati, puoi ridurre il tempo impiegato dagli utenti per rispondere a un evento di emergenza e risolverlo. Ciò può comportare una riduzione dei tempi di inattività e una maggiore disponibilità dei servizi forniti ai clienti.

- È possibile tenere traccia di ogni richiesta di accesso di emergenza e rilevare e segnalare i casi di tentativi non autorizzati di uso improprio del processo per eventi non di emergenza.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

La presente sezione fornisce indicazioni per la creazione di processi di accesso di emergenza per diverse modalità di errore relative ai carichi di lavoro implementati su AWS, a partire da linee guida comuni applicabili a tutte le modalità di errore fino a linee guida specifiche in base al tipo di errore.

Linee guida comuni per tutte le modalità di errore

Nella progettazione di un processo di accesso di emergenza per una modalità di errore, tieni presente quanto segue:

- Documenta prerequisiti e presupposti del processo: quando il processo deve e non deve essere utilizzato. Aiuta a descrivere in dettaglio la modalità di errore e a documentare le ipotesi, come lo stato di altri sistemi correlati. Ad esempio, il processo per la modalità di errore 2 presuppone che il gestore dell'identità digitale sia disponibile, ma la configurazione in AWS è stata modificata o è scaduta.
- Crea preliminarmente le risorse necessarie per il processo di accesso di emergenza (SEC10-BP05). Ad esempio, crea preliminarmente l'accesso di emergenza a un Account AWS con ruoli e utenti IAM e in tutti gli account del carico di lavoro creando ruoli IAM multi-account. Ciò assicura che queste risorse siano pronte e disponibili quando si verifica un evento di emergenza. Creando in modo preliminare le risorse, non si dipende dalle API del piano di controllo (control-plane) AWS (utilizzate per creare e modificare risorse AWS) che potrebbero non essere disponibili in caso di emergenza. Inoltre, creando in modo preliminare le risorse IAM, non è necessario tenere conto dei potenziali ritardi dovuti all'eventuale consistenza.
- Includi i processi di accesso di emergenza nei tuoi piani di gestione degli incidenti (SEC10-BP02). Documenta le modalità in cui si tiene traccia degli eventi di emergenza e come questi vengono comunicati ad altri membri dell'organizzazione, come i team di pari livello, la leadership e, se applicabile, esternamente ai clienti e ai partner aziendali.
- Definisci il processo di richiesta di accesso di emergenza nel tuo sistema di flusso di lavoro esistente, se ne hai uno, per le richieste di assistenza. In genere, tali sistemi di flusso di lavoro consentono di creare moduli di acquisizione per raccogliere informazioni sulla richiesta, tenere traccia della richiesta in ogni fase del flusso di lavoro e aggiungere passaggi di approvazione

automatici e manuali. Collega ciascuna richiesta a un evento di emergenza corrispondente tracciato nel tuo sistema di gestione degli incidenti. Disporre di un sistema uniforme per gli accessi di emergenza consente di tenere traccia di tali richieste in un unico sistema, analizzare le tendenze di utilizzo e migliorare i processi.

- Verifica che i processi di accesso di emergenza possano essere avviati solo da utenti autorizzati e richiedano l'approvazione di colleghi o manager dell'utente, a seconda dei casi. Il processo di approvazione deve funzionare in modo efficacie sia all'interno sia al di fuori dell'orario lavorativo. Definisci in che modo le richieste di approvazione possono essere eseguite da approvatori secondari, qualora gli approvatori principali non fossero disponibili, e come vengono inoltrate lungo la catena di gestione fino all'approvazione.
- Implementa affidabili meccanismi di registrazione dei log, monitoraggio e avviso per il processo e i meccanismi di accesso di emergenza. Genera log di audit dettagliati per tutti i tentativi riusciti e non riusciti di ottenere l'accesso di emergenza. Metti in correlazione l'attività con gli eventi di emergenza in corso dal sistema di gestione degli incidenti e attiva gli avvisi quando le azioni si verificano al di fuori dei periodi previsti o quando l'account di accesso di emergenza viene utilizzato durante le normali operazioni. L'account di accesso di emergenza deve essere utilizzato solo in caso di emergenza, poiché le procedure break-glass possono essere considerate una backdoor. Effettua l'integrazione con lo strumento di gestione delle informazioni e degli eventi di sicurezza (SIEM) o con AWS Security Hub CSPM per segnalare e verificare tutte le attività durante il periodo di accesso di emergenza. Quando torni alla normale operatività, effettua la rotazione automatica delle credenziali di accesso di emergenza e informa i team interessati.
- Testa periodicamente i processi di accesso di emergenza per verificare che i passaggi siano chiari e garantire il livello di accesso corretto in modo rapido ed efficiente. I processi di accesso di emergenza devono essere testati nell'ambito delle simulazioni di risposta agli incidenti (SEC10-BP07) e dei test di disaster recovery (REL13-BP03).

Modalità di errore 1: il gestore dell'identità digitale utilizzato per la federazione dell'accesso ad AWS non è disponibile

Come illustrato in SEC02-BP04 Fai affidamento su un gestore dell'identità digitale centralizzato, ti consigliamo di affidarti a un gestore dell'identità digitale centralizzato per federare gli utenti della tua forza lavoro e garantire loro l'accesso agli Account AWS. È possibile federare l'accesso a più Account AWS all'interno dell'organizzazione AWSutilizzando il Centro identità IAM oppure federare l'accesso individuale agli Account AWS utilizzando IAM. In entrambi i casi, gli utenti della forza lavoro si autenticano con il gestore dell'identità digitale centralizzato prima di essere reindirizzati a un endpoint di accesso AWS per l'autenticazione unica.

Nell'improbabile eventualità che il gestore dell'identità digitale centralizzato non sia disponibile, gli utenti della tua forza lavoro non possono federarsi per accedere agli Account AWS o gestire i propri carichi di lavoro. In questo evento di emergenza, puoi fornire un processo di accesso di emergenza secondo cui un piccolo gruppo di amministratori può accedere agli Account AWS per eseguire attività urgenti per le quali non è possibile attendere che i tuoi gestori delle identità digitali centralizzati tornino online. Ad esempio, il tuo gestore dell'identità digitale non è disponibile per 4 ore e durante quel periodo devi modificare i limiti massimi di un gruppo Amazon EC2 Auto Scaling in un account di produzione per gestire un picco imprevisto nel traffico dei clienti. Gli amministratori di emergenza devono seguire la procedura di accesso di emergenza per accedere a un Account AWS di produzione specifico e apportare le modifiche necessarie.

Il processo di accesso di emergenza si basa su un accesso di emergenza a un Account AWS creato preliminarmente, utilizzato esclusivamente per questo tipo di accessi e dispone di risorse AWS (come ruoli e utenti IAM) per supportare il processo di accesso di emergenza. Durante le normali operazioni, nessuno deve accedere all'account di accesso di emergenza ed è necessario monitorare e fornire avvisi riguardo a usi impropri di questo account (per maggiori dettagli, vedi la sezione precedente Linee guida comuni).

L'account di accesso di emergenza dispone di ruoli IAM di accesso di emergenza con autorizzazioni per assumere ruoli multi-account negli Account AWS che richiedono l'accesso di emergenza. Questi ruoli IAM sono creati preliminarmente e configurati con policy di attendibilità che valutano i ruoli IAM dell'account di emergenza come attendibili.

Per il processo di accesso di emergenza è possibile utilizzare uno dei seguenti approcci:

- Puoi creare in modo preliminare un set di utenti IAM per gli amministratori di emergenza nell'account di accesso di emergenza con password complesse e token MFA associati. Tali utenti IAM dispongono delle autorizzazioni per assumere i ruoli IAM che consentono l'accesso multi-account all'Account AWS per cui è richiesto l'accesso di emergenza. Ti consigliamo di creare il minor numero possibile di utenti di questo tipo e di assegnare ogni utente a un unico amministratore di emergenza. Durante un'emergenza, un utente amministratore di emergenza accede all'account di accesso di emergenza utilizzando la propria password e il codice token MFA, passa al ruolo IAM di accesso di emergenza nell'account di emergenza e infine passa al ruolo IAM di accesso di emergenza nell'account del carico di lavoro per eseguire l'azione di modifica di emergenza. Il vantaggio di questo approccio è che ogni utente IAM è assegnato a un amministratore di emergenza e puoi sapere quale utente ha effettuato l'accesso esaminando gli eventi CloudTrail. Lo svantaggio è che è necessario mantenere più utenti IAM con le relative password di lunga durata e i token MFA associati.

- Puoi usare l'accesso di emergenza dell'utente root Account AWS per accedere all'account di emergenza, assumere il ruolo IAM per l'accesso di emergenza e poi il ruolo multi-account nell'account del carico di lavoro. È consigliabile impostare una password sicura e più token MFA per l'utente root. Consigliamo inoltre di archiviare la password e i token MFA in un archivio di credenziali aziendali sicuro, che applichi policy di autenticazione e autorizzazione avanzate. Proteggi i fattori di reimpostazione della password e del token MFA: imposta l'indirizzo e-mail dell'account su una lista di distribuzione e-mail monitorata dagli amministratori della sicurezza del cloud e il numero di telefono dell'account su un numero di telefono condiviso anch'esso monitorato dagli amministratori della sicurezza. Il vantaggio di questo approccio è l'esistenza di un solo set di credenziali utente root da gestire. Lo svantaggio è che, trattandosi di un utente condiviso, più amministratori hanno la possibilità di accedere come utente root. Controlla gli eventi del log del tuo vault aziendale per identificare quale amministratore ha utilizzato la password dell'utente root.

Modalità di errore 2: la configurazione del gestore dell'identità digitale in AWS è stata modificata o è scaduta

Per consentire agli utenti della tua forza lavoro di effettuare l'accesso federato agli Account AWS, puoi configurare il Centro identità IAM con un gestore dell'identità digitale esterno o un gestore dell'identità digitale IAM (SEC02-BP04). In genere, la configurazione si effettua importando un documento XML di metadati SAML fornito dal gestore dell'identità digitale. Il documento XML di metadati include un certificato X.509 corrispondente a una chiave privata utilizzata dal gestore dell'identità digitale per firmare le sue asserzioni SAML.

Queste configurazioni lato AWS possono essere modificate o eliminate per errore da un amministratore. In un altro scenario, può accadere che il certificato X.509 importato in AWS sia scaduto e che un nuovo XML di metadati con un nuovo certificato non sia ancora stato importato in AWS. In entrambi gli scenari, la federazione degli utenti della forza lavoro per accedere ad AWS può essere interrotta, creando così una situazione di emergenza.

In un caso di emergenza di questo tipo, puoi fornire agli amministratori delle identità l'accesso ad AWS per risolvere i problemi di federazione. Ad esempio, l'amministratore delle identità utilizza la procedura di accesso di emergenza per accedere a un Account AWS, passa a un ruolo nell'account amministratore del Centro identità e riattiva la federazione aggiornando la configurazione del gestore dell'identità digitale esterno e importando l'ultimo documento XML di metadati SAML rilasciato dal gestore dell'identità digitale. Una volta ristabilita la federazione, gli utenti della forza lavoro continuano a utilizzare il normale processo operativo per federare l'accesso ai propri account di carico di lavoro.

È possibile seguire gli approcci illustrati nella sezione precedente Modalità di errore 1 per creare un processo di accesso di emergenza. Puoi concedere le autorizzazioni con il privilegio minimo agli amministratori delle identità per accedere solo all'account amministratore di Centro identità ed eseguire azioni in Centro identità in quell'account.

Modalità di errore 3: blocco del Centro identità

Nell'improbabile eventualità di un blocco del Centro identità IAM o una Regione AWS, ti consigliamo di eseguire una configurazione per fornire l'accesso temporaneo alla Console di gestione AWS.

Il processo di accesso di emergenza utilizza la federazione diretta rilasciata dal gestore dell'identità digitale a un IAM per accedere a un account di emergenza. Per informazioni dettagliate sul processo e sulle considerazioni di progettazione, consulta Set up emergency access to the Console di gestione AWS.

Passaggi dell'implementazione

Passaggi comuni per tutte le modalità di errore

- Crea un Account AWS dedicato per gli accessi di emergenza. Crea preliminarmente le risorse IAM necessarie nell'account, come i ruoli IAM o gli utenti IAM, e, in modo facoltativo, i gestori delle identità digitali IAM. Inoltre, crea preliminarmente ruoli IAM multi-account negli Account AWS del carico di lavoro dotati di relazioni di fiducia con i ruoli IAM corrispondenti nell'account di accesso di emergenza. Puoi usare CloudFormation StackSets con AWS Organizations per creare tali risorse negli account dei membri della tua organizzazione.

- Crea una policy di controllo dei servizi AWS Organizations per negare l'eliminazione e la modifica dei ruoli IAM multi-account negli Account AWS dei membri.
- Abilita CloudTrail per l'accesso di emergenza a un Account AWS e invia gli eventi di trail a un bucket S3 centrale nella raccolta di log relativa all'Account AWS. Se utilizzi AWS Control Tower per configurare e gestire il tuo ambiente AWS multi-account, ogni account che crei utilizzando AWS Control Tower o a cui ti iscrivi in AWS Control Tower presenta CloudTrail abilitato per impostazione predefinita e viene inviato a un bucket S3 in un Account AWS con archivio di log dedicato.
- Monitora l'attività dell'account di accesso di emergenza creando regole EventBridge coerenti con l'accesso alla console e all'attività dell'API da parte dei ruoli IAM di emergenza. Invia notifiche al tuo centro operativo di sicurezza quando si verificano attività al di fuori di un evento di emergenza in corso e di cui hai traccia nel tuo sistema di gestione degli incidenti.

Passaggi aggiuntivi per la Modalità di errore 1: il gestore dell'identità digitale utilizzato per la federazione dell'accesso ad AWS non è disponibile; per la Modalità di errore 2: la configurazione del gestore dell'identità digitale su AWS è stata modificata o è scaduta

- Crea preliminarmente le risorse in base al meccanismo scelto per l'accesso di emergenza:
  - Usando gli utenti IAM: crea preliminarmente gli utenti IAM con password complesse e dispositivi MFA associati.
  - Utilizzando l'utente utente root dell'account di emergenza: configura l'utente root con una password sicura e archivia la password nel tuo vault di credenziali aziendali. Associa più dispositivi MFA fisici all'utente root e archivia i dispositivi in posizioni a cui i membri del team di amministrazione delle emergenze possono accedere rapidamente.

Passaggi aggiuntivi per la Modalità di errore 3: blocco del Centro identità

- Come illustrato in Set up emergency access to the Console di gestione AWS, per l'accesso di emergenza a un Account AWS, crea un gestore dell'identità digitale IAM per abilitare la federazione SAML diretta dal tuo gestore dell'identità digitale.
- Crea gruppi operativi di emergenza nel tuo IdP senza membri.
- Crea ruoli IAM corrispondenti ai gruppi operativi di emergenza nell'account di accesso di emergenza.

Risorse

Best practice Well-Architected correlate:

- SEC02-BP04 Fai affidamento su un gestore dell'identità digitale centralizzato
- SEC03-BP02 Concessione dell'accesso con privilegio minimo
- SEC10-BP02 Sviluppo di piani di gestione degli incidenti
- SEC10-BP07 Esecuzione di giornate di gioco

Documenti correlati:

- Set up emergency access to the Console di gestione AWS
- Enabling SAML 2,0 federated users to access the Console di gestione AWS
- Break glass access

Video correlati:

- AWS re:Invent 2022 - Simplify your existing workforce access with IAM Identity Center
- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) deep dive

Esempi correlati:

- AWS Break Glass Role
- AWS Framework per playbook per i clienti
- AWS incident response playbook samples

SEC03-BP04 Riduzione delle autorizzazioni in modo continuo

Man mano che i team determinano gli accessi necessari, rimuovi le autorizzazioni non necessarie e stabilisci processi di revisione per ottenere le autorizzazioni con il privilegio minimo. Monitora costantemente e rimuovi le identità e le autorizzazioni inutilizzate per l'accesso sia umano che delle macchine.

Risultato desiderato: le policy di autorizzazione rispettano il principio del privilegio minimo. Man mano che le mansioni e i ruoli vengono definiti meglio, è necessario rivedere le policy di autorizzazione per eliminare le autorizzazioni non necessarie. Questo approccio riduce la portata dell'impatto nel caso di esposizione accidentale delle credenziali o di accesso in altro modo senza autorizzazione.

Anti-pattern comuni:

- L'impostazione predefinita è la concessione delle autorizzazioni di amministratore agli utenti.
- Creazione di policy eccessivamente permissive, ma senza privilegi completi di amministratore.
- Mantenimento delle policy di autorizzazione anche quando non sono più necessarie.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all’implementazione

Quando i team e i progetti sono in fase iniziale, è possibile usare policy di autorizzazione permissiva per stimolare l'innovazione e l'agilità. Ad esempio, in un ambiente di sviluppo o di test, gli sviluppatori possono avere accesso a un'ampia gamma di servizi AWS. Si consiglia di valutare in modo costante

gli accessi e di limitare l'accesso solo ai servizi e alle azioni di servizio necessari per completare il lavoro in corso. Raccomandiamo questa valutazione sia per l'identità umana che per quella macchina. Le identità macchina, talvolta chiamate account di sistema o di servizio, sono identità che consentono ad AWS di accedere ad applicazioni o server. Questo accesso è particolarmente importante in un ambiente di produzione, dove autorizzazioni troppo permissive possono avere un ampio impatto e potenzialmente esporre i dati dei clienti.

AWS offre diversi metodi per identificare utenti, ruoli, autorizzazioni e credenziali non utilizzati. AWS può anche aiutare ad analizzare l'attività di accesso di ruoli e utenti IAM, comprese le chiavi di accesso associate, e l'accesso alle risorse AWS, come gli oggetti nei bucket Amazon S3. La generazione di policy di AWS Identity and Access Management Access Analyzer può aiutare a creare policy di autorizzazione restrittive in base ai servizi e alle azioni effettive con cui interagisce un principale. Il controllo degli accessi basato su attributi (ABAC) consente di semplificare la gestione delle autorizzazioni, offrendo la possibilità di fornire le autorizzazioni agli utenti sulla base dei loro attributi anziché allegare le policy di autorizzazione direttamente a ciascun utente.

Passaggi dell’implementazione

- Usa AWS Identity and Access Management Access Analyzer: IAM Access Analyzer aiuta a identificare le risorse dell'organizzazione e gli account, ad esempio i bucket Amazon Simple Storage Service (Amazon S3) o i ruoli IAM, condivisi con un'entità esterna.
- Utilizza la generazione di policy di IAM Access Analyzer: la generazione di policy di IAM Access Analyzer consente di creare policy di autorizzazione granulari basate sull'attività di accesso di ruoli o utenti IAM.
- Esegui il test delle autorizzazioni in ambienti di livello inferiore prima della produzione: inizia utilizzando gli ambienti sandbox e di sviluppo meno critici per testare le autorizzazioni richieste per le varie funzioni lavorative utilizzando Sistema di analisi degli accessi AWS IAM. Quindi, limita e convalida progressivamente queste autorizzazioni negli ambienti di test, controllo qualità e gestione temporanea prima di applicarle in produzione. Gli ambienti di livello inferiore possono avere inizialmente autorizzazioni più permissive, poiché le policy di controllo dei servizi (SCP) applicano dei guardrail limitando il numero massimo di autorizzazioni concesse.
- Determina un periodo di tempo e una policy di utilizzo accettabili per ruoli e utenti IAM: utilizza il timestamp dell'ultimo accesso per identificare utenti e ruoli non utilizzati e rimuoverli. Rivedi le informazioni sull'ultimo accesso al servizio e sull'ultima azione per identificare e definire le autorizzazioni per specifici utenti e ruoli. Ad esempio, puoi utilizzare le informazioni sull'ultimo accesso per identificare le azioni specifiche di Amazon S3 richieste dal ruolo dell'applicazione e delimitare l'accesso del ruolo solo a tali azioni. Le funzionalità relative alle informazioni sull'ultimo

accesso sono disponibili nella Console di gestione AWS e consentono di incorporarle in modo programmatico nei flussi di lavoro dell'infrastruttura e negli strumenti automatizzati.

- Prendi in considerazione la possibilità di creare log degli eventi relativi ai dati in AWS CloudTrail: per impostazione predefinita, CloudTrail non crea log degli eventi relativi ai dati come le attività a livello di oggetto di Amazon S3 (ad esempio, `GetObject` e `DeleteObject`) o le attività delle tabelle Amazon DynamoDB (ad esempio `PutItem` e `DeleteItem`). Considera l'uso della creazione di log di questi eventi per stabilire quali utenti e ruoli devono accedere a specifici oggetti Amazon S3 o elementi di tabelle DynamoDB.

Risorse

Documenti correlati:

- Grant least privilege
- Rimuovere credenziali non necessarie
- What is AWS CloudTrail?
- Lavorare con le policy
- Logging and monitoring DynamoDB
- Abilitare la creazione di log di eventi CloudTrail per bucket e oggetti Amazon S
- Recupero dei report delle credenziali per l Account AWS

Video correlati:

- Become an IAM Policy Master in 60 Minutes or Less
- Separation of Duties, Least Privilege, Delegation, and CI/CD
- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) deep dive

SEC03-BP05 Definizione dei guardrail per le autorizzazioni dell'organizzazione

Utilizza i guardrail delle autorizzazioni per ridurre l'ambito delle autorizzazioni disponibili concedibili ai principali. La catena di valutazione delle policy di autorizzazione comprende i guardrail così da determinare le autorizzazioni effettive di un principale quando adotta decisioni relative alle autorizzazioni. È possibile definire i guardrail utilizzando un approccio basato sui livelli. Applica alcuni

guardrail in modo esteso all'intera organizzazione e applicane altri in modo granulare alle sessioni di accesso temporaneo.

Risultato desiderato: hai un chiaro isolamento degli ambienti utilizzando Account AWS separati. Le policy di controllo dei servizi (SCP) consentono di definire i guardrail delle autorizzazioni a livello di organizzazione. I guardrail più estesi sono impostati ai livelli gerarchici più vicini alla radice dell'organizzazione, mentre i guardrail più rigidi sono impostati più vicino al livello dei singoli account.

Se supportate, le policy sulle risorse definiscono le condizioni che un principale deve soddisfare per ottenere l'accesso a una risorsa. Le policy per le risorse, inoltre, definiscono l'insieme delle azioni consentite, laddove appropriato. I limiti delle autorizzazioni sono posti sui principali che gestiscono le autorizzazioni del carico di lavoro, delegando la gestione delle autorizzazioni ai singoli proprietari del carico di lavoro.

Anti-pattern comuni:

- Creare membri di Account AWS all'interno di un'organizzazione AWS, senza utilizzare SCP per limitare l'uso e le autorizzazioni disponibili alle relative credenziali root.
- Assegnare le autorizzazioni in base al privilegio minimo, senza però porre guardrail sull'insieme massimo di autorizzazioni concedibili.
- Affidarsi alla base di rifiuto implicito di AWS IAM per limitare le autorizzazioni, confidando nel fatto che le policy non concedano un'autorizzazione esplicita indesiderata.
- Eseguire più ambienti di carico di lavoro nello stesso Account AWS e affidarsi quindi a meccanismi come VPC, tag o policy sulle risorse per applicare i limiti delle autorizzazioni.

Vantaggi derivanti dall'adozione di questa best practice: i guardrail di autorizzazione contribuiscono a creare la certezza che le autorizzazioni indesiderate non possano essere concesse, anche quando una policy di autorizzazione tenta di farlo. Ciò può semplificare la definizione e la gestione delle autorizzazioni riducendo l'ambito massimo delle autorizzazioni da prendere in considerazione.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all’implementazione

Ti consigliamo di utilizzare un approccio basato sui livelli per definire i guardrail di autorizzazione per la tua organizzazione. Questo approccio riduce in modo sistematico il set massimo di autorizzazioni possibili con l'applicazione di livelli aggiuntivi. Ciò consente di concedere l'accesso in base al principio

del privilegio minimo, riducendo il rischio di accessi non intenzionali dovuti a un'errata configurazione delle policy.

Il primo passo per definire i guardrail delle autorizzazioni è isolare i carichi di lavoro e gli ambienti in Account AWS separati. I principali di un account non possono accedere alle risorse di un altro account senza l'autorizzazione esplicita in tal senso, anche se entrambi gli account fanno parte della stessa organizzazione AWS o della stessa unità organizzativa. Puoi utilizzare le unità organizzative per raggruppare gli account che desideri amministrare come una singola unità.

Il passaggio successivo consiste nel ridurre il set massimo di autorizzazioni che è possibile concedere ai principali all'interno degli account dei membri dell'organizzazione. A tale scopo, puoi utilizzare le policy di controllo dei servizi, applicabili a un'unità organizzativa o a un account. Le policy di controllo dei servizi possono applicare controlli di accesso comuni, ad esempio limitare l'accesso a Regioni AWS specifiche, aiutare a prevenire l'eliminazione di risorse o disabilitare azioni di servizio potenzialmente rischiose. Le policy di controllo dei servizi applicate alla radice dell'organizzazione influiscono solo sugli account dei membri, non sull'account di gestione. Le policy di controllo dei servizi regolano solo i principali all'interno della tua organizzazione. Le tue policy di controllo dei servizi non regolano i principali esterni alla tua organizzazione che accedono alle tue risorse.

Se utilizzi AWS Control Tower, puoi sfruttare i controlli e le zone di destinazione come base per i guardrail delle autorizzazioni e l'ambiente multi-account. Le zone di destinazione forniscono un ambiente di base preconfigurato e sicuro, con account separati per diversi carichi di lavoro e applicazioni. I guardrail impongono controlli obbligatori su sicurezza, operazioni e conformità attraverso una combinazione di policy di controllo dei servizi, regole AWS Config e altre configurazioni. Tuttavia, quando si utilizzano guardrail e zone di destinazione di Control Tower insieme a SCP personalizzati dell'organizzazione, è fondamentale seguire le best practice descritte nella documentazione AWS per evitare conflitti e garantire una governance adeguata. Per suggerimenti dettagliati sulla gestione di SCP, account e unità organizzative (UO) in un ambiente Control Tower, fai riferimento alla guida di AWS Control Tower per AWS Organizations.

Se ti attieni a queste linee guida, puoi sfruttare efficacemente i guardrail, le zone di destinazione e gli SCP personalizzati di Control Tower, riducendo al contempo i potenziali conflitti e garantendo una governance e un controllo adeguati sull'ambiente AWS multi-account.

Un ulteriore passo consiste nell'utilizzare le policy delle risorse IAM per definire le azioni disponibili che puoi intraprendere sulle risorse da esse governate, oltre a tutte le condizioni che il principale che agisce deve soddisfare. Questo può essere un ambito ampio, come consentire tutte le azioni fintanto che il principale fa parte dell'organizzazione (utilizzando la chiave di condizione PrincipalOrgId), o

granulare, come consentire solo azioni specifiche da parte di un ruolo IAM specifico. Puoi adottare un approccio simile con le condizioni nelle policy di attendibilità del ruolo IAM. Se una policy di attendibilità di una risorsa o di un ruolo nomina esplicitamente un principale nello stesso account del ruolo o della risorsa che governa, tale principale non ha bisogno di una policy IAM associata che conceda le stesse autorizzazioni. Se il principale si trova in un account diverso dalla risorsa, deve disporre di una policy IAM associata che conceda tali autorizzazioni.

Spesso, un team addetto al carico di lavoro vorrà gestire le autorizzazioni richieste dal proprio carico di lavoro. Ciò potrebbe richiedere al team di creare nuovi ruoli IAM e policy di autorizzazione. Puoi definire l'ambito massimo di autorizzazioni che il team può concedere in un limite delle autorizzazioni IAM e associare questo documento a un ruolo IAM, utilizzabile dal team per gestire autorizzazioni e ruoli IAM. Questo approccio può fornire la flessibilità necessaria per completare il lavoro, mitigando al contempo i rischi legati all'accesso amministrativo IAM.

Un passaggio più granulare consiste nell'implementazione delle tecniche di gestione degli accessi privilegiati (PAM) e di gestione temporanea degli accessi elevati (TEAM). Un esempio di gestione degli accessi privilegiati consiste nel richiedere ai principali di eseguire l'autenticazione a più fattori prima di intraprendere azioni privilegiate. Per ulteriori informazioni, consulta Configuring MFA-protected API access. La gestione temporanea degli accessi elevati richiede una soluzione che gestisca l'approvazione e i tempi in cui un principale può avere un accesso elevato. Un approccio consiste nell'aggiungere temporaneamente il principale alla policy di attendibilità dei ruoli per un ruolo IAM con accesso elevato. Un altro approccio consiste nel ridurre, in condizioni di funzionamento normale, le autorizzazioni concesse a un principale da un ruolo IAM mediante una policy di sessione, quindi revocare in modo temporaneo questa restrizione durante la finestra temporale approvata. Per ulteriori informazioni sulle soluzioni convalidate da AWS e da alcuni partner selezionati, consulta Temporary elevated access.

Passaggi dell'implementazione

1. Isola i carichi di lavoro e gli ambienti in Account AWS separati.
2. Usa le policy di controllo del servizio per ridurre il set massimo di autorizzazioni che possono essere concesse ai principali all'interno degli account membri della tua organizzazione.
   a. Quando si definiscono SCP per ridurre l'insieme massimo di autorizzazioni che possono essere concesse ai principali all'interno degli account membri dell'organizzazione, è possibile scegliere tra un approccio di tipo elenco di consentiti o elenco di rifiuto. La strategia dell'elenco di consentiti specifica esplicitamente gli accessi consentiti e blocca implicitamente tutti gli altri accessi. La strategia dell'elenco di rifiuto specifica esplicitamente gli accessi non consentiti e consente tutti gli altri accessi per impostazione predefinita. Entrambe le strategie presentano

vantaggi e compromessi e la scelta appropriata dipende dai requisiti specifici e dal modello di rischio dell'organizzazione. Per maggiori dettagli, consulta Strategy for using SCPs.

b. Inoltre, esamina gli esempi di policy di controllo dei servizi per capire come creare le SCP in modo efficace.

3. Utilizza le policy relative alle risorse IAM per definire l'ambito e specificare le condizioni per le azioni consentite sulle risorse. Utilizza le condizioni nelle policy di fiducia dei ruoli IAM per creare restrizioni all'assunzione dei ruoli.
4. Assegna limiti delle autorizzazioni IAM ai ruoli IAM che i team del carico di lavoro possono quindi utilizzare per autorizzazioni e ruoli IAM del proprio carico di lavoro.
5. Valuta le soluzioni PAM e TEAM in base alle tue esigenze.

Risorse

Documenti correlati:

- Data perimeters on AWS
- Establish permissions guardrails using data perimeters
- Logica di valutazione delle policy

Esempi correlati:

- Service control policy examples

Strumenti correlati:

- AWS Solution: Temporary Elevated Access Management
- Validated security partner solutions for TEAM

SEC03-BP06 Gestione degli accessi in base al ciclo di vita

Monitora e regola le autorizzazioni concesse ai tuoi principali (utenti, ruoli e gruppi) durante il loro ciclo di vita all'interno dell'organizzazione. Adatta le appartenenze ai gruppi quando gli utenti cambiano ruolo e rimuovi l'accesso quando un utente lascia l'organizzazione.

Risultato desiderato: monitori e modifichi le autorizzazioni durante l'intero ciclo di vita dei principali all'interno dell'organizzazione, riducendo così il rischio di privilegi superflui. Concedi

l'accesso appropriato quando crei un utente. L'accesso viene modificato man mano che cambiano le responsabilità dell'utente e lo si rimuove quando l'utente non è più attivo o ha lasciato l'organizzazione. Gestisci a livello centrale le modifiche ai tuoi utenti, ruoli e gruppi. Utilizza l'automazione per propagare le modifiche agli ambienti AWS.

Anti-pattern comuni:

- Concedere in anticipo alle identità privilegi di accesso eccessivi o ampi, al di là di quanto richiesto inizialmente.
- Non rivedere né modificare i privilegi di accesso in base al cambiamento dei ruoli e delle responsabilità delle identità nel tempo.
- Lasciare le identità inattive o terminate con privilegi di accesso attivi. Ciò aumenta il rischio di accessi non autorizzati.
- Non sfruttare l'automazione per gestire il ciclo di vita delle identità.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

Gestisci e adatta attentamente i privilegi di accesso che concedi alle identità (come utenti, ruoli, gruppi) durante il loro ciclo di vita. Questo ciclo di vita include la fase iniziale di onboarding, i continui cambiamenti di ruoli e responsabilità e l'eventuale offboarding o cessazione. Gestisci in modo proattivo l'accesso in base alla fase del ciclo di vita per mantenere il livello di accesso appropriato. Rispetta il principio del privilegio minimo per ridurre il rischio di privilegi di accesso eccessivi o non necessari.

Puoi gestire il ciclo di vita degli utenti IAM direttamente all'interno dell'Account AWS o tramite federazione dal gestore dell'identità digitale della forza lavoro al Centro identità AWS IAM. Per gli utenti IAM, puoi creare, modificare ed eliminare gli utenti e le relative autorizzazioni associate nell'Account AWS. Per gli utenti federati, puoi utilizzare il Centro identità IAM per gestire il ciclo di vita sincronizzando le informazioni sugli utenti e sui gruppi dal gestore dell'identità digitale dell'organizzazione mediante il protocollo System for Cross-domain Identity Management (SCIM).

SCIM è un protocollo standard aperto per il provisioning e il deprovisioning automatici delle identità degli utenti su diversi sistemi. Integrando il tuo gestore dell'identità digitale con il Centro identità IAM tramite SCIM, puoi sincronizzare in automatico le informazioni sugli utenti e sui gruppi, verificando che i privilegi di accesso siano concessi, modificati o revocati in base ai cambiamenti nella fonte di identità autorevole dell'organizzazione.

Man mano che i ruoli e le responsabilità dei dipendenti cambiano all'interno dell'organizzazione, modifica di conseguenza i loro privilegi di accesso. Puoi utilizzare i set di autorizzazioni del Centro identità IAM per definire diversi ruoli o responsabilità lavorative e associarli alle policy IAM e alle autorizzazioni appropriate. Quando il ruolo di un dipendente cambia, puoi aggiornare il set di autorizzazioni assegnato per riflettere le nuove responsabilità. Verifica che il dipendente disponga dell'accesso necessario rispettando il principio del privilegio minimo.

Passaggi dell'implementazione

1. Definisci e documenta un processo del ciclo di vita della gestione degli accessi, comprese le procedure per la concessione dell'accesso iniziale, le revisioni periodiche e l'offboarding.
2. Implementa ruoli IAM, gruppi e limiti delle autorizzazioni per gestire l'accesso collettivamente e applicare i livelli di accesso massimi consentiti.
3. Effettua l'integrazione con un gestore dell'identità digitale federato (come Microsoft Active Directory, Okta, Ping Identity) come fonte autorevole per le informazioni sugli utenti e sui gruppi utilizzando il Centro identità IAM.
4. Utilizza il protocollo SCIM per sincronizzare le informazioni su utenti e gruppi dal gestore dell'identità digitale nell'Identity Store del Centro identità IAM.
5. Crea set di autorizzazioni nel Centro identità IAM che rappresentino diversi ruoli o responsabilità all'interno dell'organizzazione. Definisci autorizzazioni e policy IAM appropriate per ogni set di autorizzazioni.
6. Implementa revisioni regolari degli accessi, la relativa revoca tempestiva e il miglioramento continuo del processo del ciclo di vita della gestione degli accessi.
7. Offri formazione e sensibilizza i dipendenti in materia di best practice sulla gestione degli accessi.

Risorse

Best practice correlate:

- SEC02-BP04 Fai affidamento su un gestore dell'identità digitale centralizzato

Documenti correlati:

- Manage your identity source
- Manage identities in IAM Identity Center
- Uso di AWS Identity and Access Management Access Analyzer

- IAM Access Analyzer policy generation

Video correlati:

- AWS re:Inforce 2023 - Manage temporary elevated access with AWS IAM Identity Center
- AWS re:Invent 2022 - Simplify your existing workforce access with IAM Identity Center
- AWS re:Invent 2022 - Harness power of IAM policies & rein in permissions w/Access Analyzer

SEC03-BP07 Analisi dell'accesso multi-account e pubblico

Monitora continuamente i risultati che evidenziano l'accesso multi-account e pubblico. Limita l'accesso multi-account e pubblico alle risorse che lo richiedono.

Risultato desiderato: conosci le risorse AWS condivise e con chi avviene la condivisione. Monitora e sottoponi costantemente ad audit le risorse condivise per verificare che siano condivise solo con i principali autorizzati.

Anti-pattern comuni:

- Assenza di un inventario delle risorse condivise.
- Mancanza di un processo di approvazione dell'accesso multi-account e dell'accesso pubblico alle risorse.

Livello di rischio associato se questa best practice non fosse adottata: basso

Guida all'implementazione

Se l'account è in AWS Organizations, puoi concedere l'accesso alle risorse all'intera organizzazione, a specifiche unità organizzative o a singoli account. Se l'account non è membro di un'organizzazione, puoi condividere le risorse con account individuali. Puoi concedere l'accesso multi-account diretto utilizzando policy basate sulle risorse, ad esempio le policy di bucket di Amazon Simple Storage Service (Amazon S3) o consentendo a un principale di un altro account di assumere un ruolo IAM nel tuo account. Quando utilizzi le policy sulle risorse, verifica che l'accesso sia concesso solo ai principali autorizzati. Definisci un processo per approvare tutte le risorse che devono essere pubblicamente disponibili.

AWS Identity and Access Management Access Analyzer utilizza una sicurezza comprovabile per identificare tutti i percorsi di accesso a una risorsa dall'esterno del proprio account. Esamina

continuamente le policy delle risorse e segnala i risultati dell'accesso multi-account e pubblico per semplificare l'analisi di accessi potenzialmente estesi. Prendi in considerazione la configurazione di IAM Access Analyzer con AWS Organizations per verificare di avere visibilità su tutti i tuoi account. IAM Access Analyzer consente inoltre di visualizzare in anteprima i risultati prima di implementare le autorizzazioni per le risorse. In questo modo è possibile verificare che le modifiche alle policy garantiscano alle risorse solo l'accesso multi-account e pubblico previsto. In caso di progettazione per l'accesso multi-account, puoi utilizzare policy di affidabilità per controllare i casi in cui è possibile assumere un ruolo. Ad esempio, puoi utilizzare la chiave di condizione `PrincipalOrgId` per negare un tentativo di assumere un ruolo al di fuori di AWS Organizations.

AWS Config è grado di segnalare le risorse non configurate correttamente. Inoltre, tramite i controlli delle policy AWS Config, rileva le risorse con l'accesso pubblico configurato. Servizi come AWS Control Tower e AWS Security Hub CSPM semplificano l'implementazione di controlli di rilevamento e guardrail in AWS Organizations per identificare e correggere le risorse pubblicamente esposte. Ad esempio, AWS Control Tower dispone di un guardrail gestito in grado di rilevare se eventuali snapshot Amazon EBS sono ripristinabili tramite Account AWS.

Passaggi dell'implementazione

- Prendi in considerazione l'utilizzo di AWS Config per AWS Organizations: AWS Config consente di aggregare gli esiti di più account all'interno di AWS Organizations in un account amministratore delegato. In questo modo, avrai una visione completa e potrai eseguire l'implementazione di Regole di AWS Config su più account per rilevare risorse accessibili al pubblico.
- Configurare AWS Identity and Access Management Access Analyzer: consente di identificare le risorse nell'organizzazione e negli account, ad esempio bucket Amazon S3 o ruoli IAM, condivise con un'entità esterna.
- Usa la riparazione automatica in AWS Config per rispondere alle modifiche nella configurazione dell'accesso pubblico dei bucket Amazon S3: puoi attivare in automatico le impostazioni di blocco dell'accesso pubblico per i bucket Amazon S3.
- Implementa monitoraggio e avvisi per stabilire se i bucket Amazon S3 sono diventati pubblici: devi disporre di monitoraggio e avvisi per stabilire se il blocco dell'accesso pubblico Amazon S3 è disattivato e se i bucket Amazon S3 diventano pubblici. Inoltre, se utilizzi AWS Organizations, puoi creare una policy di controllo dei servizi che impedisca modifiche alle policy di accesso pubblico di Amazon S3. AWS Trusted Advisorverifica la presenza di bucket di Amazon S3 dotati di autorizzazioni di accesso aperte. Le autorizzazioni bucket che concedono, caricano o eliminano l'accesso per chiunque danno origine a potenziali problemi di sicurezza, consentendo a chiunque di aggiungere, modificare o rimuovere elementi in un bucket. Il controllo di Trusted Advisor esamina

le autorizzazioni bucket esplicite e le policy associate che possono prevalere sulle autorizzazioni bucket. Puoi anche utilizzare AWS Config per monitorare l'accesso pubblico ai bucket Amazon S3. Per ulteriori informazioni, consulta How to Use AWS Config to Monitor for and Respond to Amazon S3 Buckets Allowing Public Access.

Quando si esaminano i controlli di accesso per i bucket Amazon S3, è importante considerare la natura dei dati memorizzati al loro interno. Amazon Macie è un servizio progettato per aiutarti a scoprire e proteggere dati sensibili, come informazioni di identificazione personale (PII), dati sanitari protetti (PHI) e credenziali come chiavi private o chiavi di accesso AWS.

Risorse

Documenti correlati:

- Using AWS Identity and Access Management Access Analyzer
- AWS Control Tower controls library
- AWS Foundational Security Best Practices standard
- AWS Config Regole gestite da
- AWS Trusted Advisor check reference
- Monitoring AWS Trusted Advisor check results with Amazon EventBridge
- Managing AWS Config Rules Across All Accounts in Your Organization
- AWS Config e AWS Organizations
- Make your AMI publicly available for use in Amazon EC2

Video correlati:

- Best Practices for securing your multi-account environment
- Dive Deep into IAM Access Analyzer

SEC03-BP08 Condivisione delle risorse in modo sicuro all'interno dell'organizzazione

Con l'aumento del numero di carichi di lavoro, è possibile che sia necessario condividere l'accesso alle risorse in tali carichi di lavoro o eseguire il provisioning delle risorse più volte su più account.

Possono esistere costrutti per segmentare il proprio l'ambiente, come ambienti di sviluppo, di test e di produzione. Tuttavia, la presenza di costrutti di separazione non limita la possibilità di condivisione sicura. La condivisione di componenti sovrapposti consente di ridurre i costi operativi e di garantire un'esperienza coerente, senza dover intuire cosa potrebbe sfuggire durante la creazione della stessa risorsa più volte.

Risultato desiderato: ridurre al minimo gli accessi involontari tramite l'uso di metodi sicuri di condivisione delle risorse all'interno dell'organizzazione e contribuire alle iniziative di prevenzione della perdita dei dati. Ridurre i costi operativi rispetto alla gestione dei singoli componenti, ridurre gli errori dovuti alla creazione manuale dello stesso componente più volte e aumentare la scalabilità dei carichi di lavoro. Si riducono i tempi di risoluzione in caso di guasti multipli e si aumenta la sicurezza nel determinare quando un componente non è più necessario. Per linee guida prescrittive sull'analisi delle risorse condivise all'esterno, consulta SEC03-BP07 Analisi dell’accesso multi-account e pubblico.

Anti-pattern comuni:

- Mancanza di un processo per il monitoraggio continuo e segnalazione automatica di condivisioni esterne inaspettate.
- Mancanza di una linea di base su ciò che deve e ciò che non deve essere condiviso.
- Scelta di una policy di ampia apertura piuttosto che di una condivisione esplicita quando richiesto.
- Creazione manuale di risorse fondamentali che si sovrappongono quando necessario.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

Progetta controlli e modelli di accesso per gestire il consumo di risorse condivise in modo sicuro e solo con entità fidate. Monitora le risorse condivise e controllane in modo costante l'accesso, ricevendo un avviso in caso di condivisione inappropriata o inaspettata. Consulta Analisi dell'accesso multi-account e pubblico per stabilire una governance che riduca l'accesso esterno alle sole risorse che lo richiedono e per stabilire un processo di monitoraggio continuo e avvisi automatici.

La condivisione tra più account all'interno di AWS Organizations è supportata da diversi servizi AWS, come AWS Security Hub CSPM, Amazon GuardDuty e AWS Backup. Questi servizi permettono di condividere i dati con un account centrale, di accedere a un account centrale o di gestire risorse e dati da un account centrale. Ad esempio, AWS Security Hub CSPM può trasferire gli esiti dai singoli account a un account centrale in cui è possibile visualizzare tutti gli esiti. AWS Backup può

eseguire un backup di una risorsa e condividerlo tra gli account. Puoi usare AWS Resource Access Manager (AWS RAM) per la condivisione di altre risorse comuni, come sottoreti VPC e collegamenti del gateway di transito alla VPN, AWS Network Firewall o pipeline IA di Amazon SageMaker.

Per limitare l'account in modo che condivida sole risorse all'interno dell'organizzazione, utilizza le policy di controllo dei servizi (SCP) per impedire l'accesso a principali esterni. In caso di condivisione di risorse, combina controlli basati sull'identità e di rete per creare un perimetro di dati per l'organizzazione e proteggere la stessa da accessi involontari. Un perimetro di dati è un insieme di guardrail preventivi che aiutano a verificare che solo le identità fidate accedano a risorse fidate dalle reti previste. Questi controlli pongono limiti adeguati alle risorse condivisibili e impediscono la condivisione o l'esposizione di risorse che non sono consentite. Ad esempio, nell'ambito del tuo perimetro di dati, puoi utilizzare le policy degli endpoint VPC e la condizione `AWS:PrincipalOrgId` per garantire che le identità che accedono ai bucket Amazon S3 appartengano alla tua organizzazione. È importante sottolineare che le SCP non si applicano a ruoli collegati a servizi o a principali dei servizi AWS.

Se usi Amazon S3, disattiva gli ACL per il bucket Amazon S3 e definisci il controllo degli accessi con le policy IAM. Per limitare l'accesso a un'origine Amazon S3 da Amazon CloudFront, effettua la migrazione dall'identità di accesso origine (OAI) al controllo di accesso origine (OAC) che supporta funzionalità aggiuntive, tra cui la crittografia lato server con AWS Key Management Service.

In alcuni casi, può essere necessario condividere le risorse al di fuori dell'organizzazione o concedere a terze parti l'accesso alle risorse stesse. Per linee guida prescrittive sulla gestione delle autorizzazioni per la condivisione esterna delle risorse, consulta Gestione delle autorizzazioni.

Passaggi dell'implementazione

1. Utilizzo di AWS Organizations - AWS Organizations è un servizio di gestione degli account che consente di consolidare più Account AWS in un'organizzazione, che è possibile creare e gestire in modo centralizzato. È possibile raggruppare gli account in unità organizzative (OU) e associare policy diverse a ciascuna di esse per soddisfare le esigenze di bilancio, sicurezza e conformità. È inoltre possibile controllare il modo in cui i servizi di Intelligenza Artificiale (IA) e di machine learning (ML) di AWS possono raccogliere e archiviare i dati e utilizzare la gestione multi-account dei servizi AWS integrati nelle organizzazioni.
2. Integrazione di AWS Organizations con i servizi AWS - Se usi un servizio AWS per eseguire attività per tuo conto negli account membri dell'organizzazione, AWS Organizations crea un ruolo collegato ai servizi IAM (SLR) per tale servizio in ogni account membro. L'accesso attendibile deve essere gestito tramite la Console di gestione AWS, le API AWS o la AWS CLI. Per linee guida

prescrittive sull'attivazione dell'accesso attendibile, consulta Using AWS Organizations with other AWS services e AWS services that you can use with Organizations.

3. Definizione di un perimetro dati - Un perimetro dati fornisce un limite ben chiaro per attendibilità e proprietà. Su AWS, solitamente è rappresentato come la tua organizzazione AWS gestita tramite AWS Organizations, insieme a eventuali sistemi o reti on-premises che accedono alle tue risorse AWS. L'obiettivo del perimetro dati è verificare che l'accesso sia consentito se l'identità è attendibile, la risorsa è attendibile e la rete è conforme. Tuttavia, la definizione di un perimetro di dati non è una soluzione adatta a tutti gli scenari. Valuta e adotta gli obiettivi di controllo delineati nel white paper Building a Perimeter on AWS in base ai tuoi specifici modelli e requisiti di rischio per la sicurezza. Devi valutare attentamente la tua specifica posizione di rischio e implementare i controlli perimetrali in linea con le tue esigenze di sicurezza.
4. Utilizzo della condivisione delle risorse nei servizi AWS e restrizioni correlate - Molti servizi AWS consentono di condividere risorse con altri account o di destinare risorse ad altri account, come ad esempio Amazon Machine Image (AMI) e AWS Resource Access Manager (AWS RAM). Limita l'API `ModifyImageAttribute` in modo da specificare gli account affidabili con cui condividere l'AMI. Specifica la condizione `ram:RequestedAllowsExternalPrincipals` in caso di utilizzo di AWS RAM per limitare la condivisione solo alla tua organizzazione e impedire l'accesso di identità non attendibili. Per considerazioni e linee guida prescrittive, consulta Resource sharing and external targets.
5. Utilizzo di AWS RAM per condividere risorse in modo sicuro all'interno di un account o con altri Account AWS - AWS RAM ti consente di condividere in modo sicuro le risorse create con i ruoli e gli utenti del tuo account e di altri Account AWS. In un ambiente multi-account, AWS RAM consente di creare una risorsa una sola volta e di condividerla con altri account. Questo approccio contribuisce a ridurre i costi operativi, fornendo al contempo coerenza, visibilità e la facilità di audit grazie alle integrazioni con Amazon CloudWatch e AWS CloudTrail, che non si ottengono quando si utilizza l'accesso multi-account.

   Se disponi di risorse condivise in precedenza mediante una policy basata sulle risorse, puoi utilizzare l'API `PromoteResourceShareCreatedFromPolicy` o un metodo equivalente per promuovere il passaggio da una condivisione di risorse a una condivisione completa di risorse completa AWS RAM.

   In alcuni casi, potrebbe essere necessario adottare ulteriori misure per condividere le risorse. Ad esempio, per condividere uno snapshot crittografato, occorre condividere una chiave AWS KMS.

Risorse

Best practice correlate:

- SEC03-BP07 Analisi dell'accesso multi-account e pubblico
- SEC03-BP09 Condivisione sicura delle risorse con terze parti
- SEC05-BP01 Creazione di livelli di rete

Documenti correlati:

- Bucket owner granting cross-account permission to objects it does not own
- How to use Trust Policies with IAM
- Building Data Perimeter on AWS
- Come utilizzare un ID esterno quando si concede a una terza parte l'accesso alle risorse AWS
- AWS services you can use with AWS Organizations
- Establishing a data perimeter on AWS: Allow only trusted identities to access company data

Video correlati:

- Granular Access with AWS Resource Access Manager
- Securing your data perimeter with VPC endpoints
- Establishing a data perimeter on AWS

Strumenti correlati:

- Esempi di policy del perimetro di dati

SEC03-BP09 Condivisione sicura delle risorse con terze parti

La sicurezza dell'ambiente cloud non si ferma alla tua organizzazione. L'organizzazione potrebbe affidare a terze parti la gestione di una parte dei dati. La gestione dei permessi per il sistema gestito da terze parti deve seguire la pratica dell'accesso just-in-time utilizzando il principio del privilegio minimo con credenziali temporanee. Lavorando a stretto contatto con una terza parte, puoi ridurre allo stesso momento la portata dell'impatto e il rischio di accesso non intenzionale.

Risultato desiderato: non vengono utilizzate credenziali AWS Identity and Access Management (IAM) a lungo termine come chiavi di accesso e chiavi segrete, poiché rappresentano un rischio per la sicurezza se utilizzate in modo improprio. Al contrario, vengono utilizzati i ruoli IAM e le credenziali temporanee per migliorare il livello di sicurezza e ridurre al minimo il sovraccarico operativo legato alla gestione delle credenziali a lungo termine. Quando concedi l'accesso a terze parti, utilizzi un identificativo univoco universale (UUID) come ID esterno nella policy di attendibilità IAM e mantieni sotto il tuo controllo le policy IAM collegate al ruolo per garantire l'accesso con il privilegio minimo. Per linee guida prescrittive sull'analisi delle risorse condivise a livello esterno, consulta SEC03-BP07 Analisi dell'accesso multi-account e pubblico.

Anti-pattern comuni:

- Utilizzo della policy di attendibilità IAM predefinita senza alcuna condizione.
- Utilizzo di credenziali IAM e chiavi di accesso a lungo termine.
- Riutilizzo di ID esterni.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

In alcuni casi, può essere necessario condividere le risorse al di fuori di AWS Organizations o concedere a terze parti l'accesso alle risorse stesse. Ad esempio, una terza parte potrebbe fornire una soluzione di monitoraggio che necessita di accedere alle risorse del tuo account. In questi casi, devi creare un ruolo IAM multi-account con i soli privilegi necessari alla terza parte. Inoltre, definisci una policy di attendibilità utilizzando la condizione ID esterno. L'utilizzo di un ID esterno da parte tua o della terza parte può comportare la generazione di un ID univoco per ogni cliente, terza parte o tenancy. Una volta creato, l'ID univoco non deve essere controllato da nessuno, se non da te. La terza parte deve implementare un processo per collegare l'ID esterno al cliente in modo sicuro, verificabile e riproducibile.

Puoi anche utilizzare IAM Roles Anywhere per la gestione dei ruoli IAM per le applicazioni all'esterno di AWS che non utilizzano API AWS.

Se la terza parte non ha più bisogno di accedere al tuo ambiente, rimuovi il ruolo. Evita di fornire a terze parti credenziali a lungo termine. Mantieni la visibilità degli altri servizi AWS che supportano la condivisione, come AWS Well-Architected Tool che consente di condividere un carico di lavoro con altri Account AWS e AWS Resource Access Manager che permette di condividere in modo sicuro una risorsa AWS di tua proprietà con altri account.

Passaggi dell'implementazione

1. Utilizza ruoli multi-account per fornire l'accesso agli account esterni. I ruoli multi-account riducono la quantità di informazioni sensibili archiviate da account esterni e terze parti per l'assistenza ai propri clienti. I ruoli multi-account consentono di concedere l'accesso alle risorse AWS dell'account in modo sicuro a terze parti, come i Partner AWS o altri account dell'organizzazione, mantenendo la possibilità di gestire e sottoporre a audit tale accesso. La terza parte può fornire il servizio da un'infrastruttura ibrida o, in alternativa, estrarre i dati in una sede esterna. IAM Roles Anywhere consente ai carichi di lavoro di terze parti di interagire in modo sicuro con i tuoi carichi di lavoro AWS e di ridurre ulteriormente la necessità di credenziali a lungo termine.

   Non devi utilizzare credenziali a lungo termine o chiavi di accesso associate agli utenti per fornire accesso ad account esterni. Per fornire l'accesso multi-account invece, occorre utilizzare i ruoli multi-account.
2. Effettua verifiche di due diligence e garantisci un accesso sicuro per i provider SaaS di terze parti. Quando condividi alcune risorse con provider SaaS di terze parti, esegui un'attenta due diligence per assicurarti che abbiano un approccio sicuro e responsabile all'accesso alle tue risorse AWS. Valuta il loro modello di responsabilità condivisa per capire quali misure di sicurezza forniscono e cosa rientra nella tua responsabilità. Assicurati che il provider SaaS disponga di un processo sicuro e verificabile per l'accesso alle tue risorse, incluso l'uso di ID esterni e principi di accesso con privilegio minimo. L'uso di ID esterni aiuta a risolvere i problemi di "confused deputy".

   Implementa controlli di sicurezza per garantire un accesso sicuro e il rispetto del principio del privilegio minimo quando concedi l'accesso a provider SaaS di terze parti. Ciò può includere l'uso di ID esterni, di identificatori univoci universali (UUID) e di policy di attendibilità IAM che limitano l'accesso solo a ciò che è strettamente necessario. Collabora a stretto contatto con il provider SaaS per stabilire meccanismi di accesso sicuri, controllarne regolarmente l'accesso alle risorse AWS e condurre audit per garantire il rispetto dei requisiti di sicurezza.
3. Rendi obsolete le credenziali a lungo termine fornite dal cliente. Rendi obsoleto l'uso di credenziali a lungo termine e utilizza ruoli multi-account oppure IAM Roles Anywhere. Se devi utilizzare credenziali a lungo termine, stabilisci un piano per migrare verso l'accesso basato sui ruoli. Per i dettagli sulla gestione delle chiavi, consulta Gestione delle identità. Collabora inoltre con il team dell'Account AWS e con la terza parte per predisporre un runbook di mitigazione dei rischi. Per un prontuario su come rispondere e mitigare il potenziale impatto di un incidente di sicurezza, consulta Risposta agli imprevisti.
4. Verifica che la configurazione presenti indicazioni prescrittive o sia automatizzata. L'ID esterno non viene trattato come un segreto, ma non deve essere un valore facilmente individuabile, come un

numero di telefono, un nome o un ID account. Rendi l'ID esterno un campo di sola lettura, in modo che non possa essere modificato per rappresentare la configurazione.

L'ID esterno può essere generato da te o dalla terza parte. Definisci un processo per stabilire chi è responsabile della generazione dell'ID. Indipendentemente dall'entità che crea l'ID esterno, la terza parte fa rispettare l'univocità e i formati in modo coerente tra i clienti.

La policy creata per l'accesso multi-account ai tuoi account deve attenersi al principio del privilegio minimo. La terza parte deve fornire un documento sulla policy del ruolo o un meccanismo di configurazione automatica che utilizzi un modello AWS CloudFormation o un equivalente per l'utente. In questo modo si riduce la possibilità di errori associati alla creazione manuale della policy e si offre un audit trail. Per ulteriori informazioni sull'utilizzo di un modello AWS CloudFormation per creare ruoli multi-account, consulta Cross-Account Roles.

La terza parte deve fornire un meccanismo di configurazione automatizzato e verificabile. Tuttavia, utilizzando il documento della policy sui ruoli che delinea gli accessi necessari, è possibile automatizzare l'impostazione del ruolo. Con un modello AWS CloudFormation o equivalente, è necessario monitorare le modifiche con il rilevamento delle deviazioni come parte della pratica di audit.

5. Tieni conto delle modifiche. La struttura del tuo account, la tua necessità di una terza parte o l'offerta di servizi che ti viene fornita possono cambiare. Occorre anticipare cambiamenti e guasti, quindi pianificare di conseguenza con le persone, i processi e le tecnologie adeguati. Sottoponi periodicamente a audit il livello di accesso fornito e implementa metodi di rilevamento per avvisare l'utente di cambiamenti inattesi. Monitora e sottoponi ad audit l'uso del ruolo e del datastore degli ID esterni. Occorre essere pronti a revocare l'accesso a terze parti, in modo temporaneo o permanente, in seguito a modifiche o modelli di accesso imprevisti. Inoltre, valuta l'impatto dell'operazione di revoca, compreso il tempo necessario per eseguirla, le persone coinvolte, il costo e l'impatto su altre risorse.

   Per linee guida prescrittive sui metodi di rilevamento, consulta le best practice di rilevamento.

Risorse

Best practice correlate:

- SEC02-BP02 Utilizzo di credenziali temporanee
- SEC03-BP05 Definizione dei guardrail per le autorizzazioni dell'organizzazione
- SEC03-BP06 Gestione degli accessi in base al ciclo di vita

- SEC03-BP07 Analisi dell'accesso multi-account e pubblico
- SEC04 Rilevamento

Documenti correlati:

- Bucket owner granting cross-account permission to objects it does not own
- How to use trust policies with IAM roles
- Delegate access across Account AWS using IAM roles
- How do I access resources in another Account AWS using IAM?
- Best practice per la sicurezza in IAM
- Cross-account policy evaluation logic
- How to use an external ID when granting access to your AWS resources to a third party
- Collecting Information from AWS CloudFormation Resources Created in External Accounts with Custom Resources
- Securely Using External ID for Accessing AWS Accounts Owned by Others
- Extend IAM roles to workloads outside of IAM with IAM Roles Anywhere

Video correlati:

- How do I allow users or roles in a separate Account AWS access to my Account AWS?
- AWS re:Invent 2018: Become an IAM Policy Master in 60 Minutes or Less
- AWS Knowledge Center Live: IAM Best Practices and Design Decisions

Esempi correlati:

- Configurazione dell'accesso multi-account in Amazon DynamoDB
- Strumento di query di rete AWS STS

Rilevamento

Il rilevamento consiste in due parti: rilevamento di modifiche della configurazione inattese o non desiderate e il rilevamento di comportamenti inattesi. Il primo può verificarsi in più luoghi in un ciclo di vita di distribuzione dell'applicazione. Utilizzando il modello Infrastructure as code (ad esempio, un modello CloudFormation), puoi verificare una configurazione non desiderata prima della distribuzione di un carico di lavoro implementando verifiche nelle pipeline CI/CD o nel controllo delle origini. Quindi, mentre implementi un carico di lavoro in ambienti di produzione e non di produzione, puoi verificare la configurazione tramite strumenti AWS nativi, open source o AWS Partner. Queste verifiche possono essere effettuate per le configurazioni che non rispettano i principi o le best practice di sicurezza o per le modifiche apportate tra il test e la distribuzione della configurazione. Per un'applicazione in esecuzione puoi verificare se la configurazione è stata modificata in modo inaspettato, al di fuori di un'implementazione nota o durante un evento di dimensionamento automatizzato.

Per la seconda parte del rilevamento, quello relativo a un comportamento inaspettato, possiamo usare strumenti o impostare un avviso al verificarsi di un aumento di un tipo particolare di chiamata API. Con Amazon GuardDuty, puoi essere avvisato se un'attività inaspettata e potenzialmente non autorizzata o dannosa si verifica all'interno dei tuoi account AWS. Devi anche monitorare in modo esplicito le chiamate API mutanti che non ti aspetti vengano utilizzate nel tuo carico di lavoro e le chiamate API che modificano l'assetto di sicurezza.

Il rilevamento consente di identificare un potenziale errore di configurazione della sicurezza, una minaccia o un comportamento imprevisto. È un aspetto fondamentale del ciclo di vita della sicurezza e può essere utilizzato per supportare un processo di qualità, un obbligo legale o di conformità, nonché per identificare e rispondere alle minacce. Esistono diversi tipi di meccanismi di rilevamento. Ad esempio, si possono analizzare i log del carico di lavoro per individuare gli exploit utilizzati. Devi esaminare regolarmente i meccanismi di rilevamento correlati al carico di lavoro per assicurarti di soddisfare le policy e i requisiti interni ed esterni. Gli avvisi e le notifiche automatizzati devono basarsi su condizioni definite per consentire ai team o agli strumenti di eseguire l'analisi. Questi meccanismi sono importanti fattori di reazione che possono aiutare l'organizzazione a identificare e comprendere l'ambito delle attività anomale.

In AWS, è possibile utilizzare diversi approcci per affrontare i meccanismi di rilevamento. Le seguenti sezioni descrivono come utilizzare questi approcci:

Best practice

- SEC04-BP01 Configurazione dei log di servizi e applicazioni

- SEC04-BP02 Acquisizione di log, esiti e metriche in posizioni standardizzate
- SEC04-BP03 Correlazione e arricchimento degli avvisi di sicurezza
- SEC04-BP04 Avvio della riparazione delle risorse non conformi

SEC04-BP01 Configurazione dei log di servizi e applicazioni

Mantieni i log degli eventi di sicurezza dei servizi e delle applicazioni. Si tratta di un principio fondamentale di sicurezza per i casi d'uso di audit, indagini e operazioni, nonché di un requisito di sicurezza comune guidato da standard, policy e procedure di governance, rischio e conformità (GRC).

Risultato desiderato: un'organizzazione deve essere in grado di recuperare in modo affidabile e coerente i log degli eventi di sicurezza da servizi e applicazioni AWS in modo tempestivo, laddove necessario, per adempiere a un processo o obbligo interno, come la risposta a un incidente di sicurezza. Considera la possibilità di centralizzare i log per migliori risultati operativi.

Anti-pattern comuni:

- Log archiviati in modo perpetuo o eliminati troppo presto.
- Tutti possono accedere ai log.
- Affidamento totale a processi manuali per la governance e l'utilizzo dei log.
- Archiviazione di ogni singolo tipo di log nel caso in cui sia necessario.
- Controllo dell'integrità del log solo quando è necessario.

Vantaggi dell'adozione di questa best practice: implementare un meccanismo di analisi della causa principale (RCA) per gli incidenti di sicurezza e una fonte di prove per gli obblighi in termini di governance, rischio e conformità.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Durante un'indagine di sicurezza o in altri casi d'uso basati sui tuoi requisiti, devi essere in grado di esaminare i log pertinenti per registrare e comprendere l'intera portata e la tempistica dell'incidente. I log sono necessari anche per la generazione di avvisi, che indicano il verificarsi di determinate azioni

di interesse. È fondamentale selezionare, attivare, memorizzare e configurare i meccanismi di query e recupero e gli avvisi.

Passaggi dell'implementazione

- Seleziona e utilizza le origini dei log. Prima di un'indagine di sicurezza, devi acquisire i log pertinenti per ricostruire in modo retroattivo l'attività in un Account AWS. Seleziona le origini dei log pertinenti per i carichi di lavoro.

  I criteri di selezione delle origini dei log devono basarsi sui casi d'uso richiesti dall'azienda. Stabilisci un percorso per ogni Account AWS utilizzando AWS CloudTrail o un percorso AWS Organizations e configura per lo stesso un bucket Amazon S3.

  AWS CloudTrail è un servizio di creazione di log che tiene traccia delle chiamate API effettuate su un Account AWS, acquisendo l'attività del servizio AWS. È attivato per impostazione predefinita, con una conservazione di 90 giorni degli eventi di gestione, recuperabili tramite la cronologia degli eventi di CloudTrail mediante Console di gestione AWS, AWS CLI o un SDK AWS. Per una maggiore conservazione e visibilità degli eventi relativi ai dati, crea un percorso CloudTrail e associalo a un bucket Amazon S3 e, facoltativamente, a un gruppo di log Amazon CloudWatch. In alternativa, puoi creare un CloudTrail Lake, che conserva i log di CloudTrail per un massimo di sette anni e fornisce una funzionalità di query basata su SQL.

  AWS consiglia ai clienti che utilizzano VPC di attivare il traffico di rete e i log DNS utilizzando rispettivamente log di flusso VPC e log delle query del risolutore Amazon Route 53 e di inviarli in streaming su un bucket Amazon S3 o un gruppo di log CloudWatch. Il log di flusso VPC può essere creato per un VPC, una sottorete o un'interfaccia di rete. Per i log di flusso VPC, puoi scegliere come e dove utilizzarli per ridurre i costi.

  I log AWS CloudTrail, i log di flusso VPC e i log delle query del risolutore Route 53 sono le origini dei log di base per supportare le indagini sulla sicurezza in AWS. Puoi anche utilizzare Amazon Security Lake per raccogliere, normalizzare e archiviare questi dati di log in formato Apache Parquet e Open Cybersecurity Schema Framework (OCSF), pronto per la query. Security Lake supporta anche altri log AWS e log provenienti da origini di terze parti.

  I servizi AWS possono generare log non acquisiti dalle origini di log di base, come log di Elastic Load Balancing, log di AWS WAF, log del registratore AWS Config, esiti di Amazon GuardDuty, log di audit di Amazon Elastic Kubernetes Service (Amazon EKS) e log del sistema operativo e delle applicazioni delle istanze Amazon EC2. Per un elenco completo delle opzioni di log e monitoraggio,

consulta l'Appendice A: definizioni delle capacità del cloud, log ed eventi della AWS Security Incident Response Guide.

- Funzionalità di log delle ricerche per ogni servizio e applicazioneAWS: ciascun servizio e applicazione AWS offre opzioni per l'archiviazione di log, ciascuna con le proprie funzionalità relative a conservazione e ciclo di vita. I due servizi di archiviazione di log più comuni sono Amazon Simple Storage Service (Amazon S3) e Amazon CloudWatch. Per lunghi periodi di conservazione, è consigliabile utilizzare Amazon S3 per la sua convenienza in termini di costi e per la flessibilità del ciclo di vita. Se l'opzione principale di log è Amazon CloudWatch Logs, puoi prendere in considerazione l'archiviazione dei log ad accesso meno frequente su Amazon S3.
- Seleziona l'archiviazione dei log: la scelta dell'archiviazione dei log è in genere correlata allo strumento di query utilizzato, alle funzionalità di conservazione, alla conoscenza e ai costi. Le opzioni principali per il log storage sono un bucket Amazon S3 o un gruppo di log CloudWatch.

  Un bucket Amazon S3 offre a possibilità di un'archiviazione economica e duratura, con una policy opzionale per il ciclo di vita. È possibile eseguire query sui log archiviati nei bucket Amazon S3 mediante servizi come Amazon Athena.

  Un gruppo di log di CloudWatch offre un'archiviazione durevole e una funzione di query integrata attraverso Approfondimenti di CloudWatch Logs.
- Identifica la conservazione dei log adeguata: se utilizzi un bucket Amazon S3 o un gruppo di log CloudWatch per archiviare i log, stabilisci cicli di vita adeguati per ogni origine di log al fine di ottimizzare i costi di archiviazione e recupero. In genere i clienti hanno a disposizione da tre mesi a un anno di log per le query, con una conservazione fino a sette anni. La scelta di disponibilità e conservazione deve essere in linea con i requisiti di sicurezza e con un insieme di mandati statutari, normativi e aziendali.
- Utilizza la registrazione per ciascun servizio e applicazione AWS con policy di conservazione e ciclo di vita adeguate: per ciascun servizio o applicazione AWS della tua organizzazione, consulta le linee guida specifiche sulla configurazione dei log:
  - Configurazione di AWS CloudTrail Trail
  - Configurazione di log di flusso VPC
  - Configurazione dell'esportazione degli esiti di Amazon GuardDuty
  - Configurazione delle registrazioni AWS Config
  - Configurazione del traffico ACL web di AWS WAF
  - Configurazione dei log del traffico di rete di AWS Network Firewall
  - Configurazione dei log di accesso per Elastic Load Balancing

  - Configurazione del log delle query del risolutore Amazon Route 53
  - Configurazione dei log di Amazon RDS
  - Configurazione dei log del piano di controllo (control-plane) di Amazon EKS
  - Configurazione dell'agente Amazon CloudWatch per istanze Amazon EC2 e server on-premises
- Seleziona e implementa meccanismi di query per i log: per le query dei log, puoi utilizzare Approfondimenti di CloudWatch Logs per i dati archiviati nei gruppi di log di CloudWatch, Amazon Athena e il Servizio OpenSearch di Amazon per i dati archiviati in Amazon S3. Inoltre, puoi utilizzare strumenti di query di terze parti, come un servizio di gestione delle informazioni e degli eventi di sicurezza (SIEM).

  Il processo di selezione di uno strumento di query dei log deve considerare gli aspetti relativi a persone, processi e tecnologia delle operazioni di sicurezza. Occorre scegliere uno strumento che soddisfi i requisiti operativi, aziendali e di sicurezza, accessibile e di cui sia possibile effettuare la manutenzione a lungo termine. Tieni presente che gli strumenti di query dei log funzionano in modo ottimale quando il numero di log da analizzare è mantenuto entro i limiti dello strumento. Non è raro avere più strumenti di query a causa di vincoli tecnici o di costo.

  Ad esempio, puoi ricorrere a uno strumento di gestione delle informazioni e degli eventi di sicurezza (SIEM) di terze parti per eseguire query sugli ultimi 90 giorni di dati, ma utilizzare Athena per eseguire query oltre i 90 giorni a causa dei costi di importazione dei log di un SIEM. Indipendentemente dall'implementazione, verifica che il tuo approccio riduca al minimo il numero di strumenti necessari per ottimizzare l'efficienza operativa, soprattutto durante le indagini su un evento di sicurezza.
- Usa i log per gli avvisi: AWS fornisce avvisi tramite diversi servizi di sicurezza:
  - AWS Config monitora e registra le configurazioni delle risorse AWS e consente di automatizzare la valutazione e la correzione rispetto alle configurazioni desiderate.
  - Amazon GuardDuty è un servizio di rilevamento delle minacce che esegue un monitoraggio continuo per individuare attività dannose e comportamenti non autorizzati al fine di proteggere carichi di lavoro e Account AWS. GuardDuty acquisisce, aggrega e analizza le informazioni dalle origini, come eventi di gestione e dati AWS CloudTrail, log DNS, log di flusso VPC e log di audit di Amazon EKS. GuardDuty estrae flussi di dati indipendenti direttamente da CloudTrail, log di flussi VPC, log di query DNS e Amazon EKS. Non è necessario gestire le policy del bucket Amazon S3 o modificare le modalità di raccolta e archiviazione dei log. È comunque consigliabile mantenere questi log a fini investigativi e di conformità.

- AWS Security Hub CSPM offre un unico punto di aggregazione, organizzazione e assegnazione di priorità per gli avvisi di sicurezza o gli esiti provenienti da diversi servizi AWS e da prodotti opzionali di terze parti per fornire una panoramica completa degli avvisi di sicurezza e dello stato di conformità.

Esistono anche motori di generazione di avvisi personalizzati per gli avvisi di sicurezza non coperti da questi servizi o per gli avvisi specifici relativi al tuo ambiente. Per informazioni sulla creazione di questi avvisi e rilevamenti, consulta la sezione Detection nella AWS Security Incident Response Guide.

Risorse

Best practice correlate:

- SEC04-BP02 Acquisizione di log, esiti e metriche in posizioni standardizzate
- SEC07-BP04 Definizione della gestione del ciclo di vita dei dati scalabili
- SEC10-BP06 Implementazione anticipata degli strumenti

Documenti correlati:

- AWS Security Incident Response Guide
- Nozioni di base su Amazon Security Lake
- Nozioni di base su Amazon CloudWatch Logs

Video correlati:

- AWS re:Invent 2022 - Introducing Amazon Security Lake

Esempi correlati:

- Assisted Log Enabler for AWS
- AWS Security Hub CSPM Findings Historical Export

SEC04-BP02 Acquisizione di log, esiti e metriche in posizioni standardizzate

I team di sicurezza si basano su log ed esiti per analizzare gli eventi che possono indicare attività non autorizzate o modifiche non intenzionali. Per semplificare tale analisi, acquisisci i log e gli esiti di sicurezza in posizioni standardizzate. Ciò rende disponibili i punti di interesse dei dati per la correlazione e può semplificare le integrazioni degli strumenti.

Risultato desiderato: un approccio standardizzato alla raccolta, analisi e visualizzazione di dati di log, esiti e metriche. I team di sicurezza possono correlare, analizzare e visualizzare in modo efficiente i dati di sicurezza su sistemi diversi per scoprire potenziali eventi di sicurezza e identificare le anomalie. I sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM) o altri meccanismi sono integrati per effettuare query e analizzare i dati dei log per risposte tempestive, tracciare ed eseguire escalation degli eventi di sicurezza.

Anti-pattern comuni:

- I team hanno e gestiscono in modo indipendente la raccolta di log e metriche che non è coerente con la strategia di registrazione dell'organizzazione.
- I team non dispongono di controlli di accesso adeguati per limitare visibilità e alterazione dei dati raccolti.
- I team non gestiscono log, esiti e metriche di sicurezza nell'ambito della loro policy di classificazione dei dati.
- I team trascurano i requisiti di sovranità e localizzazione dei dati durante la configurazione delle raccolte di dati.

Vantaggi dell'adozione di questa best practice: una soluzione di log standardizzata per raccogliere ed effettuare query su dati ed eventi dei log garantisce approfondimenti migliori ricavati dalle informazioni in essi contenute La configurazione di un ciclo di vita automatizzato per i dati di log raccolti può ridurre i costi sostenuti per l'archiviazione dei log. È possibile creare un controllo degli accessi granulare per le informazioni di log raccolte, in base a sensibilità dei dati e modelli di accesso richiesti dai team. Puoi integrare strumenti per correlare, visualizzare e ricavare informazioni dai dati.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

La crescita dell'utilizzo di AWS all'interno di un'organizzazione comporta un numero crescente di carichi di lavoro e ambienti distribuiti. Dato che ciascuno di questi carichi di lavoro e ambienti genera dati sull'attività al suo interno, l'acquisizione e l'archiviazione di questi dati a livello locale rappresenta una sfida per le operazioni di sicurezza. I team addetti alla sicurezza utilizzano strumenti come i sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM) per raccogliere dati da origini distribuite e sottoporli a flussi di lavoro di correlazione, analisi e risposta. Ciò richiede la gestione di una serie complessa di autorizzazioni per l'accesso alle varie origini dati e un sovraccarico aggiuntivo nel funzionamento dei processi di estrazione, trasformazione e caricamento (ETL).

Per superare queste sfide, valuta la possibilità di aggregare tutte le origini pertinenti dei dati dei log di sicurezza in un account Log Archive, come illustrato in Organizing Your AWS Environment Using Multiple Accounts. Ciò comprende tutti i dati relativi alla sicurezza provenienti da carichi di lavoro e log generati dai servizi AWS, come AWS CloudTrail, AWS WAF, Elastic Load Balancing e Amazon Route 53. L'acquisizione di questi dati in posizioni standardizzate e in un Account AWS separato con autorizzazioni tra account adeguate presenta diversi vantaggi. Questa pratica aiuta a prevenire la manomissione dei log all'interno di ambienti e carichi di lavoro compromessi, fornisce un unico punto di integrazione per strumenti aggiuntivi, oltre a offrire un modello più semplificato per la configurazione della conservazione dei dati e del ciclo di vita. Valuta gli impatti della sovranità dei dati, degli ambiti di conformità e di altre normative per determinare se sono necessarie più sedi di archiviazione di dati di sicurezza e relativi periodi di conservazione.

Per semplificare acquisizione e standardizzazione di log ed esiti, prendi in considerazione Amazon Security Lake nel tuo account Log Archive. Puoi configurare Security Lake in modo che importi in automatico dati da origini comuni come CloudTrail, Route 53, Amazon EKS e flussi di log VPC. Puoi anche configurare AWS Security Hub CSPM come origine dati in Security Lake, in modo da correlare gli esiti di altri servizi AWS, come Amazon GuardDuty e Amazon Inspector, con i tuoi dati di log. Puoi anche utilizzare integrazioni di origini dati di terze parti o configurare origini dati personalizzate. Tutte le integrazioni standardizzano i dati nel formato Open Cybersecurity Schema Framework (OCSF) e la relativa archiviazione avviene in bucket Amazon S3 come file Parquet, così da eliminare la necessità di elaborazione ETL.

L'archiviazione dei dati di sicurezza in posizioni standardizzate offre funzionalità di analisi avanzate. AWS consiglia di implementare strumenti per l'analisi della sicurezza operanti in un ambiente AWS in un account Security Tooling separato dal proprio account Log Archive. Questo approccio consente di implementare controlli approfonditi per proteggere l'integrità e la disponibilità dei log e del processo di gestione dei log, distinti dagli strumenti che vi accedono. Prendi in

considerazione l'utilizzo di servizi, come Amazon Athena, per l'esecuzione di query su richiesta che mettono in correlazione più origini dati. Puoi anche integrare strumenti di visualizzazione, come Quick. Le soluzioni basate sull'intelligenza artificiale sono sempre più disponibili e possono svolgere funzioni quali la traduzione degli esiti in sintesi leggibili dall'uomo e l'interazione in linguaggio naturale. Queste soluzioni sono spesso più facilmente integrate grazie a una posizione di archiviazione di dati standardizzata per le interrogazioni.

Passaggi dell'implementazione

1. Crea gli account di archiviazione di log e Security Tooling
    a. Mediante AWS Organizations, crea gli account Log Archive e Security Tooling in un'unità organizzativa di sicurezza. Se utilizzi AWS Control Tower per gestire la tua organizzazione, gli account Log Archive e Security Tooling vengono creati in automatico. Configura ruoli e autorizzazioni per l'accesso a questi account e la loro amministrazione, come richiesto.
2. Configurazione delle posizioni standardizzate dei dati di sicurezza
    a. Determina la tua strategia per la creazione di posizioni di dati di sicurezza standardizzate. Puoi raggiungere questo obiettivo mediante opzioni come approcci architetturali comuni per i data lake, prodotti per dati di terze parti o Amazon Security Lake. AWS consiglia di acquisire i dati di sicurezza da Regioni AWS che hai specificato per i tuoi account, anche in caso di mancato utilizzo attivo.
3. Configura la pubblicazione delle origini dati nelle tue posizioni standardizzate
    a. Identifica le origini per i tuoi dati di sicurezza e configurale per la pubblicazione in posizioni standardizzate. Valuta le opzioni per l'esportazione automatica dei dati nel formato desiderato anziché in quelle in cui è necessario sviluppare processi ETL. Amazon Security Lake ti consente di raccogliere dati da origini AWS supportate e sistemi integrati di terze parti.
4. Configura gli strumenti per l'accesso alle tue posizioni standardizzate
    a. Configura strumenti come Amazon Athena, Quick o soluzioni di terze parti per disporre dell'accesso necessario alle tue posizioni standardizzate. Configura questi strumenti in modo che operino dall'account Security Tooling con accesso in lettura trasversale all'account Log Archive, se applicabile. Crea abbonati in Amazon Security Lake così da fornire a questi strumenti l'accesso ai dati.

Risorse

Best practice correlate:

- SEC01-BP01 Separazione dei carichi di lavoro tramite account
- SEC07-BP04 Definizione della gestione del ciclo di vita dei dati
- SEC08-BP04 Applicazione del controllo degli accessi
- OPS08-BP02 Analizza i log relativi ai carichi di lavoro

Documenti correlati:

- Whtepaper AWS: Organizing Your AWS Environment Using Multiple Accounts
- Guida prescrittiva AWS: AWS Security Reference Architecture (AWS SRA)
- AWS Guida prescrittiva : Logging and monitoring guide for application owners

Esempi correlati:

- Aggregazione, ricerca e visualizzazione dei dati di log da origini distribuite con Amazon Athena e Quick
- Come visualizzare gli esiti di Amazon Security Lake con Quick
- Generate AI powered insights for Amazon Security Lake using Amazon SageMaker AI Studio and Amazon Bedrock
- Identify cybersecurity anomalies in your Amazon Security Lake data using Amazon SageMaker
- Ingest, transform, and deliver events published by Amazon Security Lake to Amazon OpenSearch Service
- Simplify AWS CloudTrail log analysis with natural language query generation in CloudTrail Lake

Strumenti correlati:

- Amazon Security Lake
- Integrazioni con i partner di Amazon Security Lake
- Open Cybersecurity Schema Framework (OCSF)
- Amazon Athena
- Rapidità
- Amazon Bedrock

SEC04-BP03 Correlazione e arricchimento degli avvisi di sicurezza

Un'attività imprevista può generare diversi avvisi di sicurezza da origini diverse, richiedendo un'ulteriore correlazione e arricchimento per la comprensione del contesto completo. Implementa correlazione e arricchimento automatizzati degli avvisi di sicurezza per un'identificazione e una risposta agli incidenti più accurate.

Risultato desiderato: mentre l'attività generano avvisi diversi all'interno di carichi di lavoro e ambienti, i meccanismi automatizzati correlano i dati e li arricchiscono con informazioni aggiuntive. Questa pre-elaborazione presenta un quadro più dettagliato dell'evento, che aiuta gli investigatori a determinare la criticità dell'evento e a stabilire se si tratta di un incidente che richiede una risposta formale. Questo processo riduce il carico sui team di monitoraggio e investigazione.

Anti-pattern comuni:

- Gruppi diversi di persone esaminano esiti e avvisi generati da sistemi differenti, a meno che i requisiti di separazione degli incarichi non impongano altrimenti.
- L'organizzazione convoglia tutti i dati di esiti e avvisi di sicurezza in posizioni standard, ma richiede agli investigatori di eseguire correlazioni e arricchimenti manuali.
- Ti affidi esclusivamente all'intelligence dei sistemi di rilevamento delle minacce per riferire sugli esiti e stabilire la criticità.

Vantaggi dell'adozione di questa best practice: riduzione del carico cognitivo complessivo e della preparazione manuale dei dati richiesta agli investigatori grazie a correlazione e arricchimento automatizzati degli avvisi. Questa pratica può ridurre il tempo necessario per determinare se l'evento rappresenta un incidente e avviare una risposta formale. Un contesto aggiuntivo consente inoltre di valutare con precisione la reale gravità di un evento, in quanto può essere superiore o inferiore a quanto suggerito da un avviso.

Livello di rischio associato se questa best practice non fosse adottata: basso

Guida all'implementazione

Gli avvisi di sicurezza possono provenire da diverse sorgenti all'interno di AWS, tra cui:

- Servizi come Amazon GuardDuty, AWS Security Hub CSPM, Amazon Macie, Amazon Inspector, AWS Config, AWS Identity and Access Management Access Analyzer e Strumento di analisi degli accessi alla rete

- Avvisi provenienti dall'analisi automatizzata dei log di servizi, infrastrutture e applicazioni AWS, ad esempio da Security Analytics per il Servizio OpenSearch di Amazon.
- Allarmi in risposta a modifiche nella tua attività di fatturazione provenienti da origini come Amazon CloudWatch, Amazon EventBridge o Budget AWS.
- Origini di terze parti come feed di intelligence sulle minacce e Soluzioni dei partner per la sicurezza da AWS Partner Network
- Contatto tramite AWS Trust & Safety o altre origini, come clienti o dipendenti interni.
- Utilizza Threat Technique Catalog by AWS (TTC) per facilitare l'identificazione e la correlazione del comportamento degli autori delle minacce attraverso l'identificazione degli indicatori di compromissione (IoC). Il TTC è un'estensione del framework MITRE ATT&CK, che classifica tutti i comportamenti e le tecniche noti e osservati degli autori di minacce rivolti alle risorse AWS.

Nella loro forma più elementare, gli avvisi contengono informazioni su chi (il principale o l'identità) sta facendo cosa (l'azione intrapresa) e cosa (le risorse interessate). Per ognuna di queste origini, individua le modalità con cui puoi creare mappature tra gli identificatori per queste identità, azioni e risorse come base per eseguire la correlazione. Ciò può avvenire integrando le origini degli avvisi con uno strumento di gestione delle informazioni e degli eventi di sicurezza (SIEM) per eseguire la correlazione automatica, creando pipeline ed elaborazioni di dati proprie o una combinazione di entrambi.

Un esempio di servizio in grado di eseguire la correlazione è Amazon Detective. Il rilevatore inserisce continuamente avvisi da varie origini AWS e da terze parti e utilizza diverse forme di intelligenza per creare un grafico visivo delle loro relazioni in modo da semplificare le indagini.

Sebbene la criticità iniziale di un avviso sia un aiuto per la definizione delle priorità, il relativo contesto di generazione ne determina la vera criticità. Ad esempio, Amazon GuardDuty può mostrare avvisi che indicano che un'istanza Amazon EC2 all'interno del tuo carico di lavoro sta eseguendo una query su un nome di dominio inaspettato. GuardDuty potrebbe assegnare una bassa criticità a questo avviso. Tuttavia, la correlazione automatica con altre attività svolte al momento dell'allarme potrebbe rivelare che diverse centinaia di istanze EC2 sono state distribuite dalla stessa identità, con un conseguente aumento dei costi operativi complessivi. In tal caso, questo contesto di eventi correlati causerebbe la visualizzazione di un nuovo avviso di sicurezza, la cui criticità potrebbe essere regolata su un livello superiore accelerando così l'esecuzione di ulteriori azioni.

Passaggi dell'implementazione

1. Identifica le origini delle informazioni sugli avvisi di sicurezza. Scopri come gli avvisi provenienti da questi sistemi rappresentano identità, azioni e risorse per determinare dove è possibile una correlazione.
2. Stabilisci un meccanismo per acquisire avvisi da diverse origini. Prendi in considerazione servizi come Security Hub CSPM, EventBridge e CloudWatch a tale scopo.
3. Identifica le origini per correlazione e arricchimento dei dati. Alcuni esempi di origini sono: AWS CloudTrail, log di flusso VPC, log del risolutore Route 53, log di infrastrutture e applicazioni. Alcuni di questi log, oppure tutti, potrebbero essere utilizzati tramite un'unica integrazione con Amazon Security Lake.
4. Integra i tuoi avvisi con le tue origini di correlazione e arricchimento dei dati per creare contesti degli eventi di sicurezza più dettagliati e stabilire le criticità.
    a. Amazon Detective, strumenti SIEM o altre soluzioni di terze parti possono eseguire in automatico un determinato livello di inserimento, correlazione e arricchimento.
    b. Puoi anche utilizzare i servizi AWS per crearne uno tuo. Ad esempio, puoi richiamare una funzione AWS Lambda per eseguire una query Amazon Athena rispetto a AWS CloudTrail o Amazon Security Lake e pubblicare i risultati su EventBridge.

Risorse

Best practice correlate:

- SEC10-BP03 Preparazione di funzionalità forensi
- OPS08-BP04 Creare avvisi fruibili
- REL06-BP03 Invio di notifiche (elaborazione e avvisi in tempo reale)

Documenti correlati:

- AWS Security Incident Response Guide

Esempi correlati:

- How to enrich AWS Security Hub CSPM findings with account metadata

Strumenti correlati:

- Amazon Detective
- Amazon EventBridge
- AWS Lambda
- Amazon Athena

SEC04-BP04 Avvio della riparazione delle risorse non conformi

I controlli investigativi possono segnalare la presenza di risorse non conformi ai requisiti di configurazione. È possibile avviare interventi correttivi definiti in modo programmatico, sia manualmente sia automaticamente, per riparare queste risorse e ridurre al minimo gli impatti potenziali. Quando definisci le correzioni in modo programmatico, puoi intraprendere azioni rapide e coerenti.

Sebbene l'automazione possa migliorare le operazioni di sicurezza, occorre implementarla e gestirla con attenzione. Implementa meccanismi di supervisione e controllo opportuni per verificare che le risposte automatizzate siano efficaci, accurate e in linea con le policy organizzative e la propensione al rischio.

Risultato desiderato: definizione di standard di configurazione delle risorse insieme a passaggi correttivi in caso di rilevamento di una mancata conformità. Dove possibile, hai definito gli interventi correttivi in modo programmatico, in modo da avviarli manualmente o attraverso l'automazione. Sono disponibili sistemi di rilevamento per identificare le risorse non conformi e pubblicare avvisi in strumenti centralizzati monitorati dal personale di sicurezza. Questi strumenti supportano l'esecuzione degli interventi correttivi programmatici, manualmente o automaticamente. Le soluzioni automatiche dispongono di meccanismi di supervisione e controllo adeguati per regolarne l'utilizzo.

Anti-pattern comuni:

- Automazione implementata, ma non si riescono a testare e convalidare a fondo le azioni correttive. Ciò può comportare conseguenze indesiderate, come l'interruzione delle operazioni aziendali legittime o l'instabilità del sistema.
- L'automazione migliora tempi e procedure di risposta, ma senza un monitoraggio adeguato e senza meccanismi che consentano l'intervento umano e la valutazione, quando necessario.
- Ci si affida esclusivamente agli interventi correttivi, senza considerarli come parte di un programma più ampio di risposta agli incidenti e di ripristino.

Vantaggi dell'adozione di questa best practice: gli interventi correttivi automatici possono rispondere alle configurazioni errate più rapidamente rispetto ai processi manuali, il che contribuisce a ridurre al minimo i potenziali impatti aziendali e a ridurre la finestra di opportunità per usi indesiderati. Nel definire gli interventi correttivi in modo programmatico, questi vengono applicate in modo coerente, il che riduce il rischio di errore umano. L'automazione è altresì in grado di gestire un volume maggiore di avvisi contemporaneamente, il che è molto importante negli ambienti che operano su larga scala.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

Come illustrato in SEC01-BP03 Identificazione e convalida degli obiettivi di controllo, servizi come AWS Config ed AWS Security Hub CSPM aiutano a monitorare la configurazione delle risorse nei tuoi account per verificarne la conformità ai tuoi requisiti. Quando vengono rilevate risorse non conformi, servizi come AWS Security Hub CSPM possono aiutare a instradare gli avvisi in modo appropriato e ad apportare le correzioni necessarie. Queste soluzioni offrono agli investigatori della sicurezza il punto centrale per il monitoraggio dei problemi e l'adozione di misure correttive.

Oltre a AWS Security Hub CSPM, AWS ha introdotto Security Hub Advanced. Questo servizio, annunciato al re:Invent 2025, trasforma il modo in cui le organizzazioni danno priorità ai problemi di sicurezza più critici e rispondono su larga scala per proteggere i propri ambienti cloud. Il Security Hub avanzato ora utilizza analisi avanzate per correlare, arricchire e dare priorità in automatico ai segnali di sicurezza in tutto l'ambiente cloud. Security Hub si integra perfettamente con Amazon GuardDuty, Amazon Inspector, Amazon Macie e AWS Security Hub CSPM Gli esiti correlati in Security Hub possono portare a un nuovo esito, chiamato esito di esposizione, che include un presunto percorso di attacco basato sulle vulnerabilità rilevate in ciascuna risorsa.

Mentre alcune situazioni di non conformità delle risorse sono uniche e la loro risoluzione richiede il giudizio umano, altre situazioni hanno una risposta standard che si può definire in maniera programmatica. Ad esempio, una risposta standard a un gruppo di sicurezza VPC configurato in modo errato potrebbe consistere nella rimozione delle regole non consentite e della notifica al proprietario. È possibile definire le risposte nelle funzioni di AWS Lambda, nei documenti di AWS Systems Manager Automation o tramite altri ambienti di codice di propria preferenza. Assicurati che l'ambiente sia in grado di autenticarsi ad AWS utilizzando un ruolo IAM con il minor numero di autorizzazioni necessarie per intraprendere un'azione correttiva.

Una volta definita la correzione desiderata, è possibile determinare i mezzi preferiti per avviarla. AWS Config può avviare le azioni correttive per tuo conto. Se utilizzi Security Hub CSPM, puoi farlo tramite

le azioni personalizzate, che pubblicano le informazioni sugli esiti in Amazon EventBridge. Una regola EventBridge può quindi avviare l'azione correttiva. Puoi configurare le correzioni tramite Security Hub CSPM in modo che l'esecuzione sia automatica o manuale.

Per le azioni correttive programmatiche, ti consigliamo di disporre di log e audit completi delle azioni intraprese e dei relativi risultati. Rivedi e analizza questi log per valutare l'efficacia dei processi automatizzati e identificare le aree di miglioramento. Acquisisci i log in Amazon CloudWatch Logs e i risultati delle azioni correttive sotto forma di note sugli esiti in Security Hub CSPM.

Parti prendendo in considerazione la risposta di sicurezza automatizzata su AWS, che offre soluzioni predefinite per risolvere gli errori di configurazione di sicurezza più comuni.

Passaggi dell'implementazione

1. Analizza e assegna priorità agli avvisi.
    a. Consolida gli avvisi di sicurezza provenienti da vari servizi AWS in Security Hub CSPM per una visibilità, una definizione delle priorità e una correzione centralizzate.
2. Sviluppa soluzioni correttive.
    a. Utilizza servizi come Systems Manager e AWS Lambda per eseguire correzioni programmatiche.
3. Configura le modalità di avvio delle correzioni.
    a. Utilizzando Systems Manager, definisci le azioni personalizzate che pubblicano gli esiti su EventBridge. Configura queste azioni in modo l'avvio avvenga manualmente o automaticamente.
    b. Puoi anche utilizzare Amazon Simple Notification Service (SNS) per inviare notifiche e avvisi alle parti interessate (come il team di sicurezza o i team di risposta agli incidenti) per l'intervento manuale o l'escalation, laddove necessario.
4. Rivedi e analizza i log delle correzioni per verificarne efficacia e miglioramenti.
    a. Invia l'output del log a CloudWatch Logs. Acquisisci i risultati come note sull'esito in Security Hub CSPM.

Risorse

Best practice correlate:

- SEC06-BP03 Riduzione della gestione manuale e dell'accesso interattivo

Documenti correlati:

- AWS Security Incident Response Guide - Detection

Esempi correlati:

- Risposta di sicurezza automatizzata su AWS
- Monitor EC2 instance key pairs using AWS Config
- Create AWS Config custom rules by using AWS CloudFormation Guard policies
- Automatically remediate unencrypted Amazon RDS DB instances and clusters

Strumenti correlati:

- AWS Systems Manager Automation
- Risposta di sicurezza automatizzata su AWS

Protezione dell'infrastruttura

La protezione dell'infrastruttura include metodologie di controllo, ad esempio la difesa avanzata, necessarie per soddisfare le best practice e gli obblighi normativi oppure organizzativi. L'utilizzo di queste metodologie è fondamentale per il successo delle operazioni continue nel cloud.

La protezione dell'infrastruttura è una parte cruciale di un programma di sicurezza delle informazioni. Assicura infatti che sistemi e servizi all'interno del carico di lavoro siano protetti contro gli accessi accidentali e non autorizzati e contro le potenziali vulnerabilità. Ad esempio, definirai dei limiti di attendibilità (quali i limiti di rete e account), la configurazione e la manutenzione della sicurezza del sistema (includendo argomenti come hardening, minimizzazione e applicazione di patch), l'autenticazione e le autorizzazioni del sistema operativo (prendendoti cura di utenti, chiavi e livelli di accesso) e altri punti appropriati di applicazione delle policy (quali firewall di applicazioni Web e/o gateway API).

Regioni, zone di disponibilità, zone locali AWS e AWS Outposts

Assicurati di conoscere regioni, zone di disponibilità, zone locali AWS e AWS Outposts, i componenti dell'infrastruttura globale AWS sicura.

AWS presenta il concetto di regione, ossia una sede fisica nel mondo dove riuniamo i data center. Ogni gruppo di data center logici viene definito zona di disponibilità (AZ). Ciascuna regione AWS si compone di numerose AZ isolate e fisicamente separate all'interno di un'area geografica. Se hai requisiti di residenza dei dati puoi scegliere la regione AWS vicina alla sede desiderata. Mantieni il controllo completo e la proprietà della regione in cui i dati sono fisicamente posizionati e questo può essere utile per soddisfare i requisiti di residenza dei dati e di conformità a livello regionale. Ciascun AZ dispone di fonti energetiche, sistemi di raffreddamento e sicurezza fisica indipendenti. In caso di suddivisione di un'applicazione in più AZ, aumentano isolamento e protezione da problematiche come interruzioni dell'alimentazione, fulmini, tornado, terremoti e altro ancora. Le AZ sono fisicamente separate da qualsiasi altra AZ da una distanza significativa (molti chilometri), sebbene siano tutte entro i 100 km (60 miglia) le une dalle altre. Tutte le AZ in una regione AWS sono interconnesse con una larghezza di banda elevata e una rete a bassa latenza, usano una fibra metropolitana dedicata e completamente ridondante con un throughput elevato e rete a bassa latenza tra le AZ. Tutto il traffico tra le AZ è crittografato. I clienti AWS focalizzati sull'alta disponibilità possono progettare le proprie applicazioni in modo da eseguirle in più AZ e raggiungere una tolleranza ai guasti ancora più elevata. AWS Le regioni soddisfano i più elevati livelli di sicurezza, conformità e protezione dei dati.

Le zone locali AWS posizionano i servizi AWS di calcolo, archiviazione, database e di altro tipo più vicino agli utenti. Le zone locali AWS semplificano l'esecuzione di applicazioni complesse che richiedono latenze di millisecondi a una sola cifra ai propri utenti finali, come la creazione di contenuti di media e intrattenimento, giochi in tempo reale, simulazioni di giacimenti, automazione di progettazione elettronica e machine learning. Ogni posizione di una zona locale AWS è un'estensione di una regione AWS, dove puoi eseguire applicazioni sensibili alla latenza, utilizzando servizi AWS come Amazon EC2, Amazon VPC, Amazon EBS, Amazon File Storage ed Elastic Load Balancing in prossimità geografica agli utenti finali. AWS Le zone locali offrono una connessione sicura e con larghezza di banda elevata tra i carichi di lavoro locali e quelli in esecuzione nella regione AWS, consentendoti di connetterti con facilità alla gamma completa dei servizi regionali tramite le stesse API e gli stessi set di strumenti.

AWS Outposts porta servizi nativi, infrastruttura e modelli operativi AWS praticamente in ogni data center, spazio in co-locazione o struttura on-premises. Puoi usare gli stessi strumenti, le stesse API e le stesse infrastrutture AWS nelle sedi on-premises e nel cloud AWS per offrire un'esperienza ibrida realmente coerente. AWS Outposts è progettato per ambienti connessi e può essere utilizzato per supportare carichi di lavoro che devono rimanere on-premises a causa della bassa latenza o delle esigenze di elaborazione dei dati in locale.

In AWS, ci sono diversi approcci alla protezione dell'infrastruttura. Le seguenti sezioni illustrano come utilizzare questi approcci.

Argomenti

Protezione delle reti

Gli utenti, sia appartenenti alla tua forza lavoro che i tuoi clienti, possono essere ovunque. Devi abbandonare i modelli tradizionali che si fidano di qualunque persona e di qualsiasi cosa acceda alla tua rete. Quando adotti il principio di applicare la sicurezza a qualsiasi livello, stai impiegando un approccio Zero Trust. La sicurezza Zero Trust è un modello in cui i componenti di applicazioni o microservizi sono considerati discreti tra loro e nessun componente o microservizio si fida di altri.

L'attenta pianificazione e la gestione della progettazione della rete costituiscono la base del modo in cui fornisci isolamento e limiti per le risorse all'interno del carico di lavoro. Poiché molte risorse

nel carico di lavoro operano in un VPC ed ereditano le proprietà di sicurezza, è fondamentale che la progettazione sia supportata da meccanismi di ispezione e protezione basati sull'automazione. Allo stesso modo, per i carichi di lavoro che operano al di fuori di un VPC, utilizzando esclusivamente servizi edge e/o serverless, le best practice si applicano in un approccio più semplificato. Consulta il documento AWS Well-Architected Serverless Applications Lens per istruzioni specifiche sulla sicurezza serverless.

Best practice

- SEC05-BP01 Creazione di livelli di rete
- SEC05-BP02 Controllo del traffico a tutti i livelli
- SEC05-BP03 Implementare la protezione basata sull'ispezione
- SEC05-BP04 Automatizza la protezione della rete

SEC05-BP01 Creazione di livelli di rete

Segmenta la topologia di rete in diversi livelli basati su raggruppamenti logici dei componenti del carico di lavoro in base alla sensibilità dei dati e ai requisiti di accesso. Distingui tra i componenti che richiedono l'accesso in entrata da Internet, come gli endpoint Web pubblici, e quelli che necessitano solo di un accesso interno, come i database.

Risultato desiderato: i livelli della rete rientrano in un approccio di difesa approfondito e integrale alla sicurezza che integra l'autenticazione delle identità e la strategia di autorizzazione dei carichi di lavoro. I livelli sono implementati in base alla sensibilità dei dati e ai requisiti di accesso, con meccanismi adeguati in termini di flusso e controllo del traffico.

Anti-pattern comuni:

- Creazione di tutte le risorse in un VPC o una sottorete unica.
- Creazione dei livelli di rete senza considerare i requisiti di sensibilità dei dati, il comportamento dei componenti o la loro funzionalità.
- Utilizzo di VPC e sottoreti come impostazioni predefinite per tutte le considerazioni relative al livello di rete senza considerare come i servizi gestiti da AWS influenzino la tua topologia.

Vantaggi dell'adozione di questa best practice: la definizione di livelli di rete è il primo passo per limitare i percorsi superflui lungo la rete, in particolare quelli che conducono a sistemi e dati critici. In tal modo gli attori non autorizzati avranno più difficoltà ad accedere alla rete e a navigare verso altre

risorse al suo interno. I livelli di rete discreti riducono l'ambito di analisi dei sistemi di ispezione, ad esempio per il rilevamento delle intrusioni o la prevenzione del malware. Di conseguenza, si riduce il potenziale di falsi positivi e il sovraccarico di elaborazione non necessario.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Quando si progetta l'architettura di un carico di lavoro, è comune separare i componenti in diversi livelli in base alle rispettive responsabilità. Ad esempio, un'applicazione Web può avere un livello di presentazione, uno di applicazione e uno di dati. È possibile adottare un approccio simile quando progetti la tua topologia di rete. I controlli di rete sottostanti possono contribuire a far rispettare i requisiti di accesso ai dati del carico di lavoro. Ad esempio, in un'architettura di applicazioni Web a tre livelli, puoi archiviare i file statici del livello di presentazione su Amazon S3 e distribuirli da una rete di distribuzione di contenuti (CDN), come Amazon CloudFront. Il livello di applicazione può avere endpoint pubblici che un Application Load Balancer (ALB) distribuisce in una sottorete pubblica Amazon VPC (simile a una zona demilitarizzata o DMZ), con servizi di backend implementati in sottoreti private. Il livello dati che funge da host per risorse come database e file system condivisi può risiedere in sottoreti private diverse dalle risorse del livello applicativo. In corrispondenza di ciascuno di questi limiti di livello (CDN, sottorete pubblica, sottorete privata), è possibile implementare controlli che consentano solo al traffico autorizzato di attraversarli.

Analogamente alla modellazione dei livelli di rete in base allo scopo funzionale dei componenti del carico di lavoro, occorre prendere in considerazione anche la sensibilità dei dati elaborati. Utilizzando l'esempio dell'applicazione Web, mentre tutti i servizi del carico di lavoro possono risiedere all'interno del livello di applicazione, servizi diversi possono elaborare dati con livelli di sensibilità differenti. In questo caso, la divisione del livello di applicazione utilizzando più sottoreti private, diversi VPC nello stesso Account AWS o persino VPC diversi in diversi Account AWS per ciascun livello di sensibilità dei dati può essere adeguata in base ai requisiti di controllo.

Un'ulteriore considerazione per i livelli di rete consiste nella coerenza del comportamento dei componenti del carico di lavoro. Continuando con l'esempio, nel livello di applicazione possono essere presenti servizi che accettano input dagli utenti finali o integrazioni di sistemi esterni intrinsecamente più rischiosi rispetto agli input di altri servizi. A titolo esemplificativo, si possono citare il caricamento di file, l'esecuzione di script di codice, la scansione di e-mail e così via. La collocazione di questi servizi nel proprio livello di rete contribuisce a creare un limite di isolamento più forte attorno a essi e può evitare che il loro comportamento unico crei falsi positivi in termini di allarmi nei sistemi di ispezione.

Nell'ambito della progettazione, prendi in considerazione in che modo l'utilizzo dei servizi AWS gestiti influenza la topologia di rete. Scopri in che modo servizi come Amazon VPC Lattice semplificano l'interoperabilità dei componenti del carico di lavoro tra i livelli di rete. In caso di utilizzo di AWS Lambda, esegui l'implementazione nelle sottoreti VPC, salvo in presenza di motivazioni contrarie specifiche. Determina dove si trovano gli endpoint VPC e semplifica con AWS PrivateLink il rispetto delle policy di sicurezza che limitano l'accesso ai gateway Internet.

Passaggi dell'implementazione

1. Rivedi l'architettura del carico di lavoro. Raggruppa in modo logico componenti e servizi in base alle funzioni che svolgono, alla sensibilità dei dati elaborati e al loro comportamento.
2. Per i componenti che rispondono alle richieste provenienti da Internet, prendi in considerazione l'utilizzo di bilanciatori del carico o altri proxy per fornire endpoint pubblici. Esamina il trasferimento dei controlli di sicurezza utilizzando servizi gestiti, come CloudFront, Gateway Amazon API, Elastic Load Balancing e AWS Amplify per l'hosting di endpoint pubblici.
3. I componenti in esecuzione in ambienti di calcolo, come istanze Amazon EC2, container AWS Fargate o funzioni Lambda, vanno implementati in sottoreti private, basate sui tuoi gruppi sin dal primo passaggio.
4. Per servizi AWS completamente gestiti, come Amazon DynamoDB, Amazon Kinesis o Amazon SQS, prendi in considerazione l'utilizzo degli endpoint VPC come impostazione predefinita per l'accesso tramite indirizzi IP privati.

Risorse

Best practice correlate:

- REL02 Come si pianifica la topologia di rete?
- PERF04-BP01 In che modo la rete influisce sulle prestazioni

Video correlati:

- AWS re:Invent 2023 - AWS networking foundations

Esempi correlati:

- Esempi di VPC

- Access container applications privately on Amazon ECS by using AWS Fargate, AWS PrivateLink, and a Network Load Balancer
- Serve static content in an Amazon S3 bucket through a VPC by using Amazon CloudFront

SEC05-BP02 Controllo del traffico a tutti i livelli

All'interno dei livelli della rete, utilizza un'ulteriore segmentazione per limitare il traffico solo ai flussi necessari per ogni carico di lavoro. In primo luogo, concentrati sul controllo del traffico tra Internet o altri sistemi esterni verso un carico di lavoro e il tuo ambiente (traffico nord-sud). Quindi, esamina i flussi tra diversi componenti e sistemi (traffico est-ovest).

Risultato desiderato: solo i flussi di rete necessari ai componenti dei tuoi carichi di lavoro possono comunicare tra loro e con i rispettivi client e con qualsiasi altro servizio da cui dipendono. La tua progettazione tiene conto di considerazioni come l'ingresso e l'uscita pubblici rispetto a quelli privati, la classificazione dei dati, le normative regionali e i requisiti di protocollo. Laddove possibile, preferisci flussi punto a punto rispetto al peering di rete come parte della progettazione secondo il principio del privilegio minimo.

Anti-pattern comuni:

- Adozione di un approccio alla sicurezza della rete basato sul perimetro e controllare il flusso di traffico solo al confine dei livelli di rete.
- Si presume che tutto il traffico all'interno di un livello di rete sia autenticato e autorizzato.
- Applicazione dei controlli al traffico in ingresso o a quello in uscita, ma non a entrambi.
- Affidamento esclusivo per l'autenticazione e l'autorizzazione del traffico ai componenti del carico di lavoro e ai controlli di rete.

Vantaggi dell'adozione di questa best practice: questa pratica consente di ridurre il rischio di movimenti non autorizzati all'interno della rete e aggiunge un ulteriore livello di autorizzazione ai carichi di lavoro. Eseguendo il controllo del flusso di traffico, è possibile limitare la portata dell'impatto di un incidente di sicurezza e velocizzare il rilevamento e la risposta.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all’implementazione

Se da un lato i livelli di rete aiutano a stabilire i limiti dei componenti del carico di lavoro che presentano una funzione, un livello di sensibilità dei dati e un comportamento simili, dall'altro

è possibile creare un livello di controllo del traffico molto più granulare utilizzando tecniche per segmentare ulteriormente i componenti all'interno di questi livelli, seguendo il principio del privilegio minimo. All'interno di AWS, i livelli di rete vengono definiti principalmente mediante sottoreti, in base agli intervalli di indirizzi IP, all'interno di un Amazon VPC. I livelli possono anche essere definiti utilizzando diversi VPC, ad esempio per raggruppare gli ambienti di microservizi per dominio aziendale. Se utilizzi più VPC, media l'instradamento utilizzando un AWS Transit Gateway. Sebbene ciò fornisca il controllo del traffico a Livello 4 (intervalli di porte e indirizzi IP) utilizzando gruppi di sicurezza e tabella di routing, puoi ottenere un ulteriore controllo utilizzando ulteriori servizi, come AWS PrivateLink, il firewall DNS del risolutore Amazon Route 53, AWS Network Firewall e AWS WAF.

Esamina e fai un inventario di flusso di dati e requisiti di comunicazione dei tuoi carichi di lavoro in termini di parti che avviano la connessione, porte, protocolli e livelli di rete. Valuta i protocolli disponibili per la creazione di connessioni e la trasmissione di dati in modo da selezionare quelli conformi ai tuoi requisiti di protezione (ad esempio, HTTPS anziché HTTP). Acquisisci questi requisiti sia ai limiti delle tue reti sia all'interno di ogni livello. Una volta identificati questi requisiti, esplora le opzioni per consentire il flusso del traffico richiesto solo in ciascun punto di connessione. È bene partire con i gruppi di sicurezza all'interno del VPC, in quanto collegabili a risorse che utilizzano un'interfaccia di rete elastica (ENI), come istanze Amazon EC2, attività Amazon ECS, pod Amazon EKS o database Amazon RDS. A differenza di un firewall Livello 4, un gruppo di sicurezza può avere una regola che consente il traffico da un altro gruppo di sicurezza in base al suo identificatore, riducendo al minimo gli aggiornamenti quando le risorse all'interno del gruppo cambiano nel tempo. Puoi anche filtrare il traffico utilizzando le regole in entrata e in uscita utilizzando i gruppi di sicurezza.

Quando il traffico si sposta tra i VPC, è comune utilizzare il peering VPC per il routing semplice o AWS Transit Gateway per il routing complesso. Questi approcci agevolano i flussi di traffico tra l'intervallo di indirizzi IP delle reti di origine e di destinazione. Tuttavia, se il tuo carico di lavoro richiede solo flussi di traffico tra componenti specifici in diversi VPC, prendi in considerazione l'utilizzo di una connessione punto a punto utilizzando AWS PrivateLink. A tal fine, individua quale servizio dovrebbe agire come produttore e quale dovrebbe agire come consumatore. Implementa un bilanciatore del carico compatibile per il produttore, attiva PrivateLink di conseguenza, quindi accetta una richiesta di connessione da parte del consumatore. Al servizio del produttore viene dunque assegnato un indirizzo IP privato dal VPC del consumatore, utilizzabile dallo stesso per effettuare richieste successive. Questo approccio riduce la necessità di eseguire il peer-to-peer delle reti. Includi i costi per l'elaborazione dei dati e il bilanciamento del carico come parte della valutazione PrivateLink.

Sebbene i gruppi di sicurezza e PrivateLink agevolino il controllo del flusso tra i componenti dei carichi di lavoro, un'altra considerazione importante riguarda come controllare a quali domini DNS le risorse possono accedere (se presenti). A seconda della configurazione DHCP dei tuoi VPC, puoi prendere in considerazione due diversi servizi AWS a tal scopo. La maggior parte dei consumatori utilizza il servizio DNS predefinito del risolutore Route 53 (chiamato anche server Amazon DNS o AmazonProvidedDNS) disponibile per i VPC all'indirizzo +2 del relativo intervallo CIDR. Con questo approccio, puoi creare regole DNS Firewall e associarle al tuo VPC per determinare quali azioni intraprendere per gli elenchi di domini che fornisci.

Se non stai utilizzando il risolutore Route 53 o se desideri integrare il Resolver con funzionalità di ispezione e controllo del flusso più approfondite oltre al filtro di dominio, prendi in considerazione l'implementazione di un AWS Network Firewall. Questo servizio ispeziona i singoli pacchetti utilizzando regole stateless o stateful per determinare se negare o consentire il traffico. Puoi adottare un approccio simile per filtrare il traffico Web in entrata verso i tuoi endpoint pubblici utilizzando AWS WAF. Per ulteriori indicazioni su questi servizi, consulta SEC05-BP03 Implementazione della protezione basata sulle ispezioni.

Passaggi dell'implementazione

1. Identifica i flussi di dati necessari tra i componenti dei tuoi carichi di lavoro.
2. Applica più controlli con un approccio di difesa approfondita per il traffico in entrata e in uscita, incluso l'uso di gruppi di sicurezza e tabelle di routing.
3. Usa i firewall per definire un controllo granulare sul traffico di rete in entrata, in uscita e attraverso i tuoi VPC, come il firewall DNS del risolutore Route 53, AWS Network Firewall e AWS WAF. Prendi in considerazione l'utilizzo di AWS Firewall Manager per configurare e gestire a livello centrale le regole del firewall in tutta l'organizzazione.

Risorse

Best practice correlate:

- REL03-BP01 Scelta del tipo di segmentazione del carico di lavoro
- SEC09-BP02 Applicazione della crittografia dei dati in transito

Documenti correlati:

- Security best practices for your VPC

- AWS Network Optimization Tips
- Guidance for Network Security on AWS
- Secure your VPC's outbound network traffic in the Cloud AWS

Strumenti correlati:

- AWS Firewall Manager

Video correlati:

- AWS Transit Gateway reference architectures for many VPCs
- Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield
- AWS re:Inforce 2023: Firewalls and where to put them

SEC05-BP03 Implementare la protezione basata sull'ispezione

Imposta i punti di ispezione del traffico tra i livelli di rete per verificare che i dati in transito corrispondano a categorie e schemi previsti. Analizza i flussi di traffico, i metadati e i modelli per identificare, rilevare e rispondere agli eventi in modo più efficace.

Risultato desiderato: ispezione e autorizzazione del traffico che attraversa i livelli di rete. Le decisioni di autorizzazione e rifiuto si basano su regole esplicite, informazioni sulle minacce e deviazioni dai comportamenti di base. Le protezioni diventano più severe man mano che il traffico si avvicina ai dati sensibili.

Anti-pattern comuni:

- Affidamento esclusivo alle regole del firewall basate su porte e protocolli. Mancato sfruttamento di sistemi intelligenti.
- Creazione di regole del firewall basate su specifici modelli di minaccia attuali, soggetti a modifiche.
- Ispezione solo del traffico che transita da una sottorete privata a una pubblica o da una sottorete pubblica a Internet.
- Mancata visione di base del traffico di rete da confrontare per individuare eventuali anomalie di comportamento.

Vantaggi dell'adozione di questa best practice: i sistemi di ispezione ti consentono di creare regole intelligenti, come consentire o negare il traffico solo in presenza di determinate condizioni all'interno dei dati di traffico. Approfitta dei set di regole gestiti AWS e dei partner, basati sulle più recenti informazioni sulle minacce, man mano che il panorama delle minacce cambia nel tempo. In questo modo si riduce l'onere di mantenere le regole e di ricercare gli indicatori di compromissione, riducendo il potenziale di falsi positivi.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

Ottieni un controllo preciso sul traffico di rete stateful e stateless utilizzando AWS Network Firewall o altri firewall e sistemi di prevenzione delle intrusioni () Marketplace AWS che puoi implementare dietro un Gateway Load Balancer (IPS). GWLBAWS Network Firewall supporta le specifiche open source compatibili con Suricata per proteggere il carico di lavoro. IPS

Sia le soluzioni dei AWS Network Firewall fornitori che utilizzano un GWLB supportano diversi modelli di implementazione dell'ispezione in linea. Ad esempio, è possibile eseguire l'ispezione su VPC base individuale, centralizzarla o implementarla in un modello ibrido in cui il traffico est-ovest attraversa un'ispezione VPC e l'ingresso di Internet viene ispezionato di conseguenza. VPC VPC Un'altra considerazione è se la soluzione supporti l'unwrapping Transport Layer Security (TLS), che consente un'ispezione approfondita dei pacchetti per i flussi di traffico avviati in entrambe le direzioni. Per ulteriori informazioni e dettagli approfonditi su queste configurazioni, consulta la AWS Network Firewall Best Practice guide.

Se utilizzate soluzioni che eseguono out-of-band ispezioni, come l'analisi pcap dei dati a pacchetto provenienti da interfacce di rete che funzionano in modalità promiscua, potete configurare il mirroring del traffico. VPC Il traffico in mirroring viene conteggiato ai fini della larghezza di banda disponibile delle interfacce ed è soggetto agli stessi costi di trasferimento dati del traffico non in mirroring. È possibile verificare se le versioni virtuali di questi dispositivi sono disponibili su Marketplace AWS, che possono supportare la distribuzione in linea dietro a. GWLB

Per i componenti che effettuano transazioni tramite protocolli HTTP basati su protocolli basati, proteggi la tua applicazione dalle minacce comuni con un firewall per applicazioni Web ()WAF. AWS WAFè un firewall per applicazioni Web che ti consente di monitorare e bloccare le richieste HTTP (S) che corrispondono alle tue regole configurabili prima di inviarle ad Amazon API Gateway CloudFront, Amazon AWS AppSync o un Application Load Balancer. Prendi in considerazione l'ispezione approfondita dei pacchetti quando valuti l'implementazione del firewall delle tue applicazioni Web,

poiché alcuni richiedono l'interruzione TLS prima dell'ispezione del traffico. Per iniziare AWS WAF, puoi utilizzare Regole gestite da AWSin combinazione con le tue integrazioni partner o utilizzare le integrazioni dei partner esistenti.

Puoi gestire centralmente AWS WAF AWS Shield Advanced AWS Network Firewall, e i gruppi di VPC sicurezza Amazon in tutta la tua AWS organizzazione con AWS Firewall Manager.

Passaggi dell'implementazione

1. Determina se puoi disciplinare le regole di ispezione in modo ampio, ad esempio attraverso un'ispezioneVPC, o se hai bisogno di un approccio più granulare. VPC
2. Per soluzioni di ispezione in linea:
   a. Se lo utilizzi AWS Network Firewall, crea regole, politiche firewall e il firewall stesso. Una volta configurati questi elementi, puoi indirizzare il traffico verso l'endpoint del firewall per consentire l'ispezione.
   b. Se utilizzi un'appliance di terze parti con un Gateway Load Balancer GWLB (), distribuisci e configura l'appliance in una o più zone di disponibilità. Quindi, crea il tuo servizio endpointGWLB, l'endpoint e configura il routing per il tuo traffico.
3. Per out-of-band le soluzioni di ispezione:
   1. Attiva il mirroring VPC del traffico sulle interfacce in cui è necessario rispecchiare il traffico in entrata e in uscita. Puoi utilizzare EventBridge le regole di Amazon per richiamare una AWS Lambda funzione per attivare il mirroring del traffico sulle interfacce quando vengono create nuove risorse. Indirizza le sessioni di mirroring del traffico al Network Load Balancer davanti all'appliance che elabora il traffico.
4. Per soluzioni di traffico Web in entrata:
   a. Per configurare AWS WAF, inizia configurando una lista di controllo degli accessi Web (web). ACL Il Web ACL è una raccolta di regole con un'azione predefinita (ALLOWoDENY) elaborata in serie che definisce il modo in cui l'utente WAF gestisce il traffico. Puoi creare regole e gruppi personalizzati o utilizzare gruppi di regole AWS gestiti nel tuo WebACL.
   b. Una volta configurato ACL il Web, associalo a una AWS risorsa (come un Application Load Balancer, un API Gateway REST API o una CloudFront distribuzione) per iniziare a proteggere il traffico Web. ACL

Risorse

Documenti correlati:

- What is Traffic Mirroring?
- Implementing inline traffic inspection using third-party security appliances
- AWS Network Firewall architetture di esempio con routing
- Architettura di ispezione centralizzata con AWS Gateway Load Balancer e AWS Transit Gateway

Esempi correlati:

- Best practices for deploying Gateway Load Balancer
- TLSconfigurazione di ispezione per il traffico in uscita crittografato e AWS Network Firewall

Strumenti correlati:

- Marketplace AWS IDS/IPS

SEC05-BP04 Automatizza la protezione della rete

Automatizza l'implementazione delle protezioni di rete utilizzando DevOps pratiche come infrastructure as code (IaC) e pipeline CI/CD. Queste pratiche possono aiutare a tenere traccia delle modifiche apportate alle protezioni di rete attraverso un sistema di controllo delle versioni, a ridurre i tempi di implementazione delle modifiche e a rilevare se le protezioni di rete si allontanano dalla configurazione desiderata.

Risultato desiderato: definizione delle protezioni di rete con modelli e relativo inserimento in un sistema di controllo delle versioni. In caso di nuove modifiche, vengono avviate pipeline automatiche che ne orchestrano test e implementazione. I controlli delle policy e altri test statici sono in atto per convalidare le modifiche prima dell'implementazione. L'implementazione delle modifiche avviene in un ambiente di staging per convalidare il funzionamento previsto dei controlli. Anche l'implementazione negli ambienti di produzione avviene in automatico una volta approvati i controlli.

Anti-pattern comuni:

- Affidamento ai singoli team del carico di lavoro la definizione dell'intero stack di rete, delle protezioni e delle automazioni. Mancata pubblicazione degli aspetti standard dello stack di rete e delle protezioni in modo centralizzato per consentire ai team del carico di lavoro di utilizzarli.
- Affidamento a un team di rete centrale per definire tutti gli aspetti della rete, delle protezioni e delle automazioni. Mancata delega degli aspetti specifici del carico di lavoro dello stack di rete e delle protezioni al team di quel carico di lavoro.

- Individuazione del giusto equilibrio tra centralizzazione e delega tra un team di rete e i team del carico di lavoro, ma mancata applicazione di standard di test e implementazione coerenti nei modelli IaC e nelle pipeline CI/CD. Mancata acquisizione delle configurazioni richieste negli strumenti che controllano l'aderenza dei modelli.

Vantaggi dell'adozione di questa best practice: l'utilizzo di modelli per definire le protezioni di rete consente di tracciare le modifiche e confrontarle nel tempo con un sistema di controllo delle versioni. L'uso dell'automazione per testare e implementare le modifiche crea standardizzazione e prevedibilità, aumentando le possibilità di una corretta implementazione e riducendo le configurazioni manuali ripetitive.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

Una serie di controlli di protezione della rete descritti in SEC05-BP02 Controllo dei flussi di traffico all'interno dei livelli di rete e SEC 05-BP03 Implementazione della protezione basata sull'ispezione sono inclusi sistemi di regole gestite che possono essere aggiornati automaticamente in base alle più recenti informazioni sulle minacce. Esempi di protezione degli endpoint Web includono regole gestite e mitigazione automatica a livello di applicazione.AWS WAFAWS Shield Advanced DDoS Utilizza i gruppi di regole AWS Network Firewall gestite per rimanere aggiornato sugli elenchi di domini con scarsa reputazione e sulle firme delle minacce.

Oltre alle regole gestite, ti consigliamo di utilizzare DevOps procedure per automatizzare la distribuzione delle risorse di rete, delle protezioni e delle regole specificate. Puoi acquisire queste definizioni in AWS CloudFormation o in un altro strumento Infrastructure as Code (IaC) di tua scelta, trasferirle in un sistema di controllo delle versioni e implementarle mediante pipeline CI/CD. Utilizzate questo approccio DevOps per ottenere i vantaggi tradizionali della gestione dei controlli di rete, come rilasci più prevedibili, test automatizzati con strumenti come AWS CloudFormation Guarde rilevamento degli scostamenti tra l'ambiente distribuito e la configurazione desiderata.

In base alle decisioni prese nell'ambito di SEC05-BP01 Create network layer, potreste avere un approccio di gestione centralizzato alla creazione VPCs dedicato ai flussi di ingresso, uscita e ispezione. Come descritto nella AWS Security Reference Architecture (AWS SRA), è possibile definirli VPCs in un account dedicato all'infrastruttura di rete. È possibile utilizzare tecniche simili per definire centralmente l'VPCsutilizzo dei carichi di lavoro in altri account, i relativi gruppi di sicurezza, le AWS Network Firewall distribuzioni, le regole di Route 53 Resolver e le configurazioni del DNS firewall e altre risorse di rete. Puoi condividere queste risorse con gli altri tuoi account con AWS

Resource Access Manager. Grazie a questo approccio, puoi semplificare test e implementazione automatici dei controlli di rete nell'account di rete, con una sola destinazione da gestire. Puoi farlo in un modello ibrido, in cui distribuisci e condividi determinati controlli centralmente e deleghi altri controlli ai singoli team del carico di lavoro e ai rispettivi account.

Passaggi dell'implementazione

1. Stabilisci quali aspetti della rete e delle protezioni sono definiti a livello centrale e quali possono essere gestiti dai tuoi team del carico di lavoro.
2. Crea ambienti per testare e implementare le modifiche alla tua rete e alle relative protezioni. Ad esempio, utilizza un account Network Testing e uno Network Production.
3. Determina come archivierai e manterrai i tuoi modelli in un sistema di controllo delle versioni. Archivia i modelli centrali in un repository distinto da quello dei carichi di lavoro, mentre i modelli dei carichi di lavoro possono essere archiviati in repository specifici per quel carico di lavoro.
4. Crea pipeline CI/CD per testare e implementare modelli. Definisci i test per verificare che non ci siano configurazioni errate e che i modelli siano conformi agli standard aziendali.

Risorse

Best practice correlate:

- SEC01-BP06 Automatizza l'implementazione dei controlli di sicurezza standard

Documenti correlati:

- AWS Security Reference Architecture - Network account

Esempi correlati:

- AWS Deployment Pipeline Reference Architecture
- NetDevSecOpsper modernizzare le AWS implementazioni di rete
- Integrazione di test e report AWS CloudFormation di sicurezza AWS Security Hub CSPMAWS CodeBuild

Strumenti correlati:

- AWS CloudFormation
- AWS CloudFormation Guard
- cfn_nag

Protezione delle risorse di calcolo

Le risorse di calcolo includono istanze EC2, container, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora. Ciascuno di questi tipi di risorse di calcolo richiede approcci di sicurezza diversi. Tuttavia, condividono strategie comuni da prendere in considerazione: difesa in profondità, gestione delle vulnerabilità, riduzione della superficie di attacco, automazione di configurazione e operatività ed esecuzione di attività a distanza. In questa sezione troverai linee guida generali per la protezione di risorse di calcolo per servizi chiave. Per ciascun servizio AWS utilizzato, è importante verificare i suggerimenti di sicurezza specifici nella documentazione del servizio.

Best practice

- SEC06-BP01 Gestione delle vulnerabilità
- SEC06-BP02 Fornitura di dati di calcolo a partire da immagini rinforzate
- SEC06-BP03 Riduzione della gestione manuale e dell'accesso interattivo
- SEC06-BP04 Convalida l'integrità del software
- SEC06-BP05 Automatizzazione della protezione delle risorse di calcolo

SEC06-BP01 Gestione delle vulnerabilità

Scansiona e correggi di frequente le vulnerabilità del codice, delle dipendenze e dell'infrastruttura per proteggerti da nuove minacce.

Risultato desiderato: disponi di una soluzione che analizza continuamente il carico di lavoro alla ricerca di vulnerabilità del software, potenziali difetti ed esposizione involontaria della rete. Hai definito processi e procedure per identificare, assegnare priorità e correggere queste vulnerabilità in base a criteri di valutazione del rischio. Inoltre, hai implementato la gestione automatizzata delle patch per le istanze di calcolo. Il programma di gestione delle vulnerabilità è integrato nel ciclo di vita di sviluppo del software, con soluzioni per la scansione del codice sorgente durante la pipeline CI/CD.

Anti-pattern comuni:

- Assenza di un programma di gestione delle vulnerabilità.

- Esecuzione di patch di sistema senza considerare gravità o prevenzione del rischio.
- Utilizzo di software che ha superato la data di fine vita (EOL) prevista dal fornitore.
- Implementazione del codice in produzione prima di aver analizzato i problemi di sicurezza.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

La gestione delle vulnerabilità è un aspetto fondamentale per mantenere un ambiente cloud sicuro e affidabile. Implica un processo completo che include scansioni di sicurezza, identificazione e definizione delle priorità dei problemi e operazioni di applicazione delle patch per risolvere le vulnerabilità identificate. L'automazione svolge un ruolo fondamentale in questo processo perché facilita la scansione continua dei carichi di lavoro alla ricerca di potenziali problemi ed esposizione involontaria della rete, nonché le operazioni di correzione.

Il modello di responsabilità condivisa di AWS è un concetto fondamentale alla base della gestione delle vulnerabilità. Secondo questo modello, AWS è responsabile della protezione dell'infrastruttura sottostante, compresi hardware, software, reti e strutture in cui vengono eseguiti i servizi AWS. D'altra parte, l'utente è responsabile della protezione dei dati, delle configurazioni di sicurezza e delle attività di gestione associate a servizi come le istanze Amazon EC2 e gli oggetti Amazon S3.

AWS offre una gamma di servizi utili per i programmi di gestione delle vulnerabilità. Amazon Inspector analizza continuamente i carichi di lavoro AWS alla ricerca di vulnerabilità del software e accessi involontari alla rete, mentre Gestione patch di AWS Systems Manager aiuta a gestire l'applicazione delle patch sulle istanze Amazon EC2. Questi servizi possono essere integrati con AWS Security Hub CSPM, un servizio di gestione del livello di sicurezza nel cloud che automatizza i controlli di sicurezza di AWS, centralizza gli avvisi di sicurezza e fornisce una visione completa del livello di sicurezza di un'organizzazione. Inoltre, Sicurezza di Amazon CodeGuru utilizza l'analisi statica del codice per identificare potenziali problemi nelle applicazioni Java e Python durante la fase di sviluppo.

Incorporando pratiche di gestione delle vulnerabilità nel ciclo di vita dello sviluppo software, puoi affrontare in modo proattivo le vulnerabilità prima che vengano introdotte negli ambienti di produzione, riducendo così il rischio di eventi di sicurezza e riducendo al minimo il potenziale impatto delle vulnerabilità.

Passaggi dell'implementazione

1. Comprendi il modello di responsabilità condivisa: consulta il modello di responsabilità condivisa di AWS per comprendere le tue responsabilità in materia di protezione dei carichi di lavoro e dei dati nel cloud. AWS è responsabile della protezione dell'infrastruttura cloud sottostante, mentre tu sei responsabile della protezione delle applicazioni, dei dati e dei servizi che utilizzi.
2. Implementa la scansione delle vulnerabilità: configura un servizio di scansione delle vulnerabilità, come Amazon Inspector, per scansionare automaticamente le istanze di calcolo (ad esempio, macchine virtuali, container o funzioni serverless) alla ricerca di vulnerabilità software, potenziali difetti ed esposizione involontaria della rete.
3. Stabilisci processi di gestione delle vulnerabilità: definisci processi e procedure per identificare, assegnare priorità e correggere le vulnerabilità. Ciò può includere la pianificazione di scansioni periodiche delle vulnerabilità, la definizione di criteri di valutazione dei rischi e l'individuazione di tempistiche di correzione in base alla gravità della vulnerabilità.
4. Configura la gestione delle patch: utilizza un servizio di gestione delle patch per automatizzare il processo di applicazione delle patch alle istanze di calcolo, sia per i sistemi operativi che per le applicazioni. Puoi configurare il servizio affinché scansioni le istanze alla ricerca di patch mancanti e installi automaticamente le patch in base a una pianificazione. Prendi in considerazione Gestione patch di AWS Systems Manager per fornire questa funzionalità.
5. Configura la protezione contro i malware: implementa meccanismi per rilevare eventuali software dannosi nel tuo ambiente. Ad esempio, puoi utilizzare strumenti come Amazon GuardDuty per analizzare e rilevare eventuali malware, nonché per notificarne la presenza nei volumi EC2 ed EBS. GuardDuty può anche scansionare gli oggetti appena caricati su Amazon S3 alla ricerca di potenziali malware o virus e intervenire per isolarli prima che vengano inseriti nei processi a valle.
6. Integra la scansione delle vulnerabilità nelle pipeline CI/CD: se utilizzi una pipeline CI/CD per l'implementazione delle applicazioni, integra gli strumenti di scansione delle vulnerabilità nella pipeline. Strumenti come Sicurezza di Amazon CodeGuru e le opzioni open source consentono di scansionare il codice sorgente, le dipendenze e gli artefatti alla ricerca di potenziali problemi di sicurezza.
7. Configura un servizio di monitoraggio della sicurezza: configura un servizio di monitoraggio della sicurezza, come AWS Security Hub CSPM, per ottenere una visione completa del tuo livello di sicurezza su più servizi cloud. Il servizio deve raccogliere gli esiti in materia di sicurezza da varie origini e presentarli in un formato standardizzato per facilitare la definizione delle priorità e la correzione.

8. Implementa test di penetrazione delle applicazioni web: se la tua applicazione è un'applicazione web e la tua organizzazione dispone delle competenze necessarie o può usufruire di assistenza esterna, valuta la possibilità di implementare dei test di penetrazione delle applicazioni web per identificare potenziali vulnerabilità nella tua applicazione.
9. Automatizza con l'infrastructure as code: utilizza strumenti di infrastructure as code (IaC), come AWS CloudFormation, per automatizzare l'implementazione e la configurazione delle risorse, inclusi i servizi di sicurezza menzionati in precedenza. Questa pratica consente di creare un'architettura delle risorse più coerente e standardizzata per più account e ambienti.
10. Monitora e migliora continuamente: monitora continuamente l'efficacia del programma di gestione delle vulnerabilità e apporta i miglioramenti necessari. Esamina gli esiti di sicurezza, valuta l'efficacia delle operazioni di correzione e adatta di conseguenza i tuoi processi e strumenti.

Risorse

Documenti correlati:

- AWS Systems Manager
- Panoramica sulla sicurezza di AWS Lambda
- Amazon CodeGuru
- Improved, Automated Vulnerability Management for Cloud Workloads with a New Amazon Inspector
- Automate vulnerability management and remediation in AWS using Amazon Inspector and AWS Systems Manager – Part 1

Video correlati:

- Securing Serverless and Container Services
- Security best practices for the Amazon EC2 instance metadata service

SEC06-BP02 Fornitura di dati di calcolo a partire da immagini rinforzate

Riduci le opportunità di accesso involontario agli ambienti di runtime implementandoli da immagini rafforzate. Acquisisci dipendenze di runtime, come immagini di container e librerie di applicazioni, solo da registri affidabili e verifica le loro firme. Crea i tuoi registri privati per archiviare immagini e librerie attendibili da utilizzare nei tuoi processi di compilazione e implementazione.

Risultato desiderato: l'allocazione delle risorse di calcolo avviene a partire da immagini di base rinforzate. Le dipendenze esterne, ad esempio immagini dei container e librerie di applicazioni, vengono recuperate solo da registri attendibili e ne vengono verificate le firme. Queste sono archiviate in registri privati a cui i processi di compilazione e implementazione possono fare riferimento. Scansiona e aggiorna con regolarità immagini e dipendenze per proteggerti da eventuali vulnerabilità scoperte di recente.

Anti-pattern comuni:

- Acquisizione di immagini e librerie da registri attendibili, ma senza verificarne la firma o eseguire scansioni delle vulnerabilità prima di metterle in uso.
- Rafforzamento delle immagini, ma senza test regolari per individuare nuove vulnerabilità o aggiornarle alla versione più recente.
- Installazione o non rimozione di pacchetti software non necessari durante il ciclo di vita previsto dell'immagine.
- Affidamento esclusivo alle patch per mantenere aggiornate le risorse di calcolo di produzione. La sola applicazione di patch può comunque far sì che nel tempo le risorse di calcolo si allontanino dallo standard rafforzato. L'applicazione delle patch può inoltre non essere in grado di rimuovere le minacce informatiche che un attore pericoloso potrebbero aver installato durante un evento di sicurezza.

Vantaggi dell'adozione di questa best practice: il rafforzamento delle immagini favorisce la riduzione del numero di percorsi disponibili nell'ambiente di runtime, che possono consentire l'accesso non intenzionale a utenti o servizi non autorizzati. Inoltre, può ridurre l'ambito dell'impatto in caso di accesso involontario.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Per rafforzare i tuoi sistemi, occorre partire dalle versioni più recenti dei sistemi operativi, delle immagini dei container e delle librerie delle applicazioni. Applica le patch ai problemi noti. Riduci al minimo il sistema rimuovendo applicazioni, servizi, driver dei dispositivi, utenti predefiniti e altre credenziali non necessari. Adotta qualsiasi altra azione necessaria, come la disabilitazione delle porte, per creare un ambiente che disponga solo delle risorse e delle capacità necessarie per i carichi di lavoro. Da questa linea di base è possibile installare software, agenti o altri processi necessari per scopi quali il monitoraggio del carico di lavoro o la gestione delle vulnerabilità.

È possibile ridurre l'onere del rafforzamento dei sistemi utilizzando le linee guida fornite da fonti attendibili, come le guide tecniche per l'implementazione della sicurezza del Center for Internet Security (CIS) e della Defense Information Systems Agency (DISA). STIGs Ti consigliamo di iniziare con una Amazon Machine Image (AMI) pubblicata da AWS o da un APN partner e utilizzare AWS EC2Image Builder per automatizzare la configurazione in base a una combinazione appropriata di CIS controlli e. STIG

Sebbene siano disponibili immagini rinforzate e ricette di EC2 Image Builder che applicano CIS i consigli DISA STIG o, è possibile che la loro configurazione impedisca il corretto funzionamento del software. In questa situazione, è possibile partire da un'immagine di base non protetta, installare il software e quindi applicare i CIS controlli in modo incrementale per testarne l'impatto. Per qualsiasi CIS controllo che impedisca l'esecuzione del software, verifica se invece riesci a implementare i consigli più dettagliati sulla protezione avanzata in un. DISA Tieni traccia dei diversi CIS controlli e DISA STIG configurazioni che riesci ad applicare con successo. Utilizzateli per definire di conseguenza le vostre ricette di rafforzamento delle EC2 immagini in Image Builder.

Per i carichi di lavoro containerizzati, le immagini rinforzate di Docker sono disponibili nell'archivio pubblico Amazon Elastic Container Registry (). ECR È possibile utilizzare EC2 Image Builder per rafforzare le immagini dei contenitori. AMIs

Analogamente ai sistemi operativi e alle immagini dei contenitori, è possibile ottenere pacchetti di codice (o librerie) da archivi pubblici, tramite strumenti come pip, npm, Maven e. NuGet Ti consigliamo di gestire i pacchetti di codice integrando repository privati, ad esempio all'interno di AWS CodeArtifact, con repository pubblici affidabili. Questa integrazione può gestire il recupero, l'archiviazione e la conservazione dei pacchetti per te. up-to-date I processi di creazione delle applicazioni possono quindi ottenere e testare la versione più recente di questi pacchetti insieme all'applicazione, utilizzando tecniche come Software Composition Analysis (SCA), Static Application Security Testing (SAST) e Dynamic Application Security Testing (DAST).

Per i carichi di lavoro serverless che utilizzano AWS Lambda, semplifica la gestione delle dipendenze dei pacchetti utilizzando i livelli Lambda. Usa i livelli Lambda per configurare un set di dipendenze standard condivise tra diverse funzioni in un archivio autonomo. È possibile creare e gestire i livelli tramite il relativo processo di compilazione, in modo da garantire la permanenza delle funzioni in modo centralizzato. up-to-date

Passaggi dell'implementazione

- Rafforzamento del sistema operativo. Utilizzate immagini di base provenienti da fonti attendibili come base per costruire il vostro hardenedAMIs. Usa EC2Image Builder per personalizzare il software installato sulle tue immagini.
- Rafforzamento delle risorse containerizzate. Configura le risorse containerizzate in modo che rispettino le best practice in materia di sicurezza. Quando utilizzi i contenitori, implementa la scansione delle ECR immagini nella tua pipeline di creazione e, su base regolare, nel tuo archivio di immagini da cercare CVEs nei contenitori.
- Quando si utilizza l'implementazione serverless con AWS Lambda, utilizza i livelli Lambda per separare il codice delle funzioni dell'applicazione e le librerie dipendenti condivise. Configura la firma del codice per Lambda così da garantire l'esecuzione del solo codice attendibile nelle funzioni Lambda.

Risorse

Best practice correlate:

- OPS05-BP05 Esegui la gestione delle patch

Video correlati:

- Approfondimento sulla sicurezza AWS Lambda

Esempi correlati:

- STIGCompatibile con la compilazione rapida con Image AMI Builder EC2
- Building better container images
- Using Lambda layers to simplify your development process
- Sviluppa e distribuisci AWS Lambda livelli utilizzando Serverless Framework
- Creazione di una pipeline end-to-end AWS DevSecOps CI/CD con strumenti e software open source SCA SAST DAST

SEC06-BP03 Riduzione della gestione manuale e dell'accesso interattivo

Utilizza l'automazione per eseguire attività di implementazione, configurazione, manutenzione e investigazione, laddove possibile. Quando l'automazione non è disponibile, considera l'accesso manuale alle risorse di calcolo in caso di procedure di emergenza o in ambienti sicuri (sandbox).

Risultato desiderato: acquisizione mediante script programmatici e documenti di automazione (runbook) delle azioni autorizzate sulle tue risorse di calcolo. Questi runbook vengono avviati in automatico, attraverso i sistemi di rilevamento delle modifiche, o manualmente, quando è necessario il giudizio umano. L'accesso diretto alle risorse di calcolo è disponibile solo in situazioni di emergenza, quando l'automazione non è disponibile. Tutte le attività manuali vengono inserite in un log e in un processo di revisione per migliorare in modo continuo le capacità di automazione.

Anti-pattern comuni:

- Accesso interattivo alle istanze Amazon EC2 con protocolli come SSH o RDP.
- Mantenimento degli accessi dei singoli utenti, come `/etc/passwd` o gli utenti locali di Windows.
- Condivisione di una password o chiave privata per accedere a un'istanza tra più utenti.
- Installazione del software e creazione o aggiornamento manuali dei file di configurazione.
- Aggiornamento o applicazione di patch manuale al software.
- Accesso a un'istanza per risolvere i problemi.

Vantaggi dell'adozione di questa best practice: l'esecuzione di azioni automatizzate favorisce la riduzione del rischio operativo legato a modifiche non intenzionali ed errori di configurazione. Abolire l'uso di Secure Shell (SSH) e Remote Desktop Protocol (RDP) per l'accesso interattivo significa ridurre la portata dell'accesso alle risorse di calcolo. In tal modo si elimina un percorso comune per le azioni non autorizzate. Acquisire le attività di gestione delle risorse di calcolo in documenti di automazione e script di programmazione significa definire e sottoporre ad audit l'intero ambito delle attività autorizzate a un livello di dettaglio granulare.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all’implementazione

L'accesso a un'istanza è un approccio classico all'amministrazione del sistema. Dopo aver installato il sistema operativo del server, gli utenti in genere accedono manualmente per configurare il sistema e installare il software desiderato. Nel corso del ciclo di vita del server, gli utenti possono accedere

per eseguire aggiornamenti del software, applicare patch, modificare le configurazioni e risolvere i problemi.

L'accesso manuale comporta tuttavia una serie di rischi. Richiede un server che ascolti le richieste, come un servizio SSH o RDP, in grado di fornire un potenziale percorso di accesso non autorizzato. Inoltre, aumenta il rischio di errore umano associato all'esecuzione di operazioni manuali. Le conseguenze possono essere incidenti sul carico di lavoro, danneggiamento o distruzione dei dati o altri problemi di sicurezza. L'accesso umano richiede inoltre protezioni contro la condivisione delle credenziali, creando ulteriori costi di gestione.

Per mitigare questi rischi, è possibile implementare una soluzione di accesso remoto basata su agenti, come AWS Systems Manager. AWS Systems Manager L'agente (SSM Agent) avvia un canale crittografato, pertanto non si avvale dell'ascolto di richieste esterne. Per stabilire questo canale su un endpoint VPC, valuta il ricorso alla configurazione di SSM Agent.

Systems Manager offre un controllo granulare delle modalità di interazione con le istanze gestite. Sei tu a definire le automazioni da eseguire, chi può eseguirle e quando possono essere eseguite. Systems Manager è in grado di applicare patch, installare software e apportare modifiche alla configurazione senza accesso interattivo all'istanza. Systems Manager può inoltre fornire l'accesso a una shell (interprete di comandi) remota e registrare ogni comando richiamato e il relativo output durante la sessione nei log e in Amazon S3. AWS CloudTrail registra le invocazioni delle API di Systems Manager per l'ispezione.

Passaggi dell'implementazione

1. Installa AWS Systems Manager Agent (SSM Agent) sulle istanze Amazon EC2. Verifica se SSM Agent è incluso e avviato in automatico nell'ambito della configurazione AMI di base.
2. Verifica che i ruoli IAM associati ai profili dei tuoi profili delle istanze EC2 includano la policy IAM gestita di `AmazonSSMManagedInstanceCore`.
3. Disabilita SSH, RDP e altri servizi di accesso remoto in esecuzione sulle tue istanze. Puoi farlo eseguendo script configurati nella sezione dei dati utente dei tuoi modelli di avvio o creando AMI personalizzate con strumenti come EC2 Image Builder.
4. Verifica che le regole di ingresso del gruppo di sicurezza applicabili alle tue istanze EC2 non consentano l'accesso sulla porta 22/tcp (SSH) o sulla porta 3389/tcp (RDP). Implementa il rilevamento e l'invio di avvisi su gruppi di sicurezza non configurati correttamente utilizzando servizi come AWS Config.
5. Definisci automazioni, runbook ed esegui comandi appropriati in Systems Manager. Utilizza le policy IAM per definire chi può eseguire queste azioni e le condizioni in base alle quali sono

consentite. Testa in modo approfondito queste automazioni in un ambiente non di produzione. Richiama queste automazioni quando necessario, invece di accedere in modo interattivo all'istanza.

6. Utilizza AWS Systems Manager Session Manager per fornire un accesso interattivo alle istanze, quando necessario. Attiva la creazione di log delle attività di sessione per mantenere un audit trail in Amazon CloudWatch Logs o Amazon S3.

Risorse

Best practice correlate:

- REL08-BP04 Esecuzione dell'implementazione utilizzando un'infrastruttura immutabile

Esempi correlati:

- Replacing SSH access to reduce management and security overhead with AWS Systems Manager

Strumenti correlati:

- AWS Systems Manager

Video correlati:

- Controlling User Session Access to Instances in AWS Systems Manager Session Manager

SEC06-BP04 Convalida l'integrità del software

Utilizza la verifica crittografica per convalidare l'integrità degli artefatti software (comprese le immagini) utilizzati dal tuo carico di lavoro. La firma crittografica del software è una tutela contro le modifiche non autorizzate eseguite negli ambienti di calcolo.

Risultato desiderato: ottenimento di tutti gli artefatti da fonti attendibili. I certificati del sito Web del fornitore sono convalidati. Gli artefatti scaricati vengono verificati a livello crittografico tramite le relative firme. Il tuo software è firmato e verificato a livello crittografico dai tuoi ambienti di elaborazione.

Anti-pattern comuni:

- Affidarsi a siti Web di fornitori attendibili per ottenere artefatti software, ma ignorare gli avvisi di scadenza dei certificati. Download senza confermare la validità dei certificati.
- Convalida dei certificati dei siti Web dei fornitori, ma senza verificare a livello crittografico gli artefatti scaricati da questi siti Web.
- Affidarsi esclusivamente a digest o hash per convalidare l'integrità del software. Gli hash stabiliscono che gli artefatti non sono stati modificati rispetto alla versione originale, ma non ne convalidano l'origine.
- Mancata firma di software, codice o librerie di proprietà, anche se utilizzati solo per le proprie implementazioni.

Vantaggi dell'adozione di questa best practice: la convalida dell'integrità degli artefatti da cui dipende il carico di lavoro consente di prevenire l'ingresso di malware negli ambienti di calcolo. La firma del software aiuta a proteggerti dall'esecuzione non autorizzata nei tuoi ambienti di calcolo. Proteggi la catena di approvvigionamento del software firmando e verificando il codice.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

Immagini del sistema operativo, immagini dei container e artefatti del codice sono spesso distribuiti con controlli di integrità disponibili, ad esempio attraverso un digest o un hash. Questi permettono ai client di verificare l'integrità elaborando il proprio hash del payload e verificando che sia uguale a quello pubblicato. Sebbene questi controlli aiutino a verificare l'assenza di manomissioni del payload, non ne convalidano la provenienza dalla fonte originale (la sua provenienza). La verifica della provenienza richiede un certificato rilasciato da un'autorità attendibile per firmare digitalmente l'artefatto.

Se utilizzi un software o artefatti scaricati nel tuo carico di lavoro, controlla se il fornitore offre una chiave pubblica per la verifica della firma digitale. Ecco alcuni esempi di come AWS fornisce una chiave pubblica e le istruzioni di verifica per il software che pubblichiamo:

- EC2Image Builder: verifica la firma del download di installazione AWS TOE
- AWS Systems Manager: verifica della firma dell'agente SSM
- Amazon CloudWatch: verifica della firma del pacco dell' CloudWatch agente

Incorpora la verifica della firma digitale nei processi utilizzati per ottenere e rafforzare le immagini, come discusso in SEC06-BP02 Provision compute from hardened images.

È possibile utilizzare AWS Signer per la gestione della verifica delle firme, nonché del ciclo di vita di firma del codice per il tuo software e i tuoi artefatti. AWS Lambda e Amazon Elastic Container Registry offrono entrambi integrazioni con Signer per verificare le firme di codice e immagini. Utilizzando gli esempi nella sezione Risorse, puoi incorporare Signer nelle tue pipeline di integrazione e distribuzione continua (CI/CD) per automatizzare la verifica delle firme e la firma del tuo codice e delle tue immagini.

Risorse

Documenti correlati:

- Cryptographic Signing for Containers
- Le migliori pratiche per proteggere la pipeline di creazione delle immagini dei container utilizzando AWS Signer
- Annuncio della firma di Container Image con AWS Signer Amazon EKS
- Configurazione della firma del codice per AWS Lambda
- Best practices and advanced patterns for Lambda code signing
- Firma del codice tramite CA AWS Certificate Manager privata e chiavi AWS Key Management Service asimmetriche

Esempi correlati:

- Automatizza la firma del codice Lambda con Amazon e CodeCatalyst AWS Signer
- Firma e convalida OCI degli artefatti con AWS Signer

Strumenti correlati:

- AWS Lambda
- AWS Signer
- AWS Certificate Manager
- AWS Key Management Service
- AWS CodeArtifact

SEC06-BP05 Automatizzazione della protezione delle risorse di calcolo

Automatizza le operazioni di protezione delle risorse di calcolo per ridurre la necessità di intervento umano. Usa la scansione automatica per rilevare potenziali problemi all'interno delle tue risorse di calcolo e rimedia con risposte programmatiche automatiche o operazioni di gestione del parco. Incorpora l'automazione nei tuoi processi CI/CD per implementare carichi di lavoro affidabili con dipendenze aggiornate.

Risultato desiderato: tutte le scansioni e le applicazioni di patch alle risorse di calcolo avvengono per mezzo di sistemi automatizzati. Utilizzi la verifica automatica per controllare che immagini e dipendenze del software provengano da origini attendibili e non siano state manomesse. Il controllo dei carichi di lavoro avviene in automatico per verificare la presenza di dipendenze aggiornate, così come la relativa firma per stabilire l'affidabilità negli ambienti di calcolo AWS. Le correzioni automatiche vengono avviate al rilevamento di risorse non conformi.

Anti-pattern comuni:

- Adozione della pratica dell'infrastruttura immutabile, senza però disporre di una soluzione di patch di emergenza o di sostituzione dei sistemi di produzione.
- Utilizzo dell'automazione per correggere le risorse non correttamente configurate, ma senza un meccanismo di annullamento manuale. Possono verificarsi situazioni in cui è necessario modificare i requisiti e sospendere le automazioni fino a quando non si modificano.

Vantaggi dell'adozione di questa best practice: riduzione del rischio di accessi alle risorse di calcolo e relativi utilizzi non autorizzati mediante l'automazione. Contribuisce a evitare che le configurazioni errate si diffondano negli ambienti di produzione e a rilevare e correggere tali configurazioni nel caso in cui si verifichino. L'automazione aiuta anche a rilevare l'accesso non autorizzato delle risorse di calcolo e il loro utilizzo, riducendo i tempi di risposta. In questo modo è possibile ridurre la portata complessiva dell'impatto del problema.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

È possibile applicare le automazioni descritte nelle pratiche del pilastro della sicurezza per proteggere le risorse di calcolo. SEC06-BP01 Gestione delle vulnerabilità illustra come utilizzare Amazon Inspector nelle pipeline CI/CD e per la scansione continua degli ambienti di runtime alla ricerca di vulnerabilità ed esposizioni comuni (CVE) note. Puoi utilizzare AWS Systems Manager per

applicare patch o eseguire nuove implementazioni da nuove immagini tramite runbook automatizzati in modo da mantenere il tuo parco di calcolo aggiornato con software e librerie più recenti. Utilizza queste tecniche per ridurre la necessità di processi manuali e l'accesso interattivo alle tue risorse di elaborazione. Consulta SEC06-BP03 Riduzione della gestione manuale e dell'accesso interattivo per scoprire di più.

L'automazione contribuisce anche all'implementazione di carichi di lavoro affidabili, come illustrato in SEC06-BP02 Provisioning di calcolo da immagini rafforzate e SEC06-BP04 Convalida dell'integrità del software. Puoi utilizzare servizi come EC2 Image Builder, AWS Signer, AWS CodeArtifact e Amazon Elastic Container Registry (ECR) per scaricare, verificare, costruire e archiviare immagini e dipendenze di codice rafforzate e approvate. Oltre a Inspector, ognuno di questi può svolgere un ruolo nel processo CI/CD, in modo che il carico di lavoro arrivi in produzione solo quando è confermato che le sue dipendenze sono aggiornate e provengono da origini affidabili. Il carico di lavoro è inoltre firmato in modo che gli ambienti di calcolo AWS, come AWS Lambda e Amazon Elastic Kubernetes Service (EKS), possano verificare l'assenza di manomissioni prima di consentirne l'esecuzione.

Oltre a questi controlli preventivi, è possibile utilizzare l'automazione nei controlli investigativi anche per le risorse di calcolo. Ad esempio, AWS Security Hub CSPM offre lo standard NIST 800-53 Rev. 5 che include controlli come le [EC2.8] EC2 le istanze devono utilizzare Instance Metadata Service versione 2 (IMDSv2).. IMDSv2 utilizza le tecniche di autenticazione della sessione, il blocco delle richieste che contengono un'intestazione X-Forwarded-For HTTP e un TTL di rete pari a 1 per bloccare il traffico proveniente da origini esterne al fine di recuperare informazioni sull'istanza EC2. Questo controllo in Security Hub CSPM può rilevare quando le istanze EC2 utilizzano IMDSv1 e avviare una riparazione automatizzata. Scopri di più su rilevamento e riparazioni automatiche in SEC04-BP04 Avvio della riparazione delle risorse non conformi.

Passaggi dell'implementazione

1. Automatizza la creazione di AMI rafforzate, conformi e consolidate con EC2 Image Builder. È possibile produrre immagini che incorporano i controlli dei benchmark del Center for Internet Security (CIS) o gli standard della Security Technical Implementation Guide (STIG) dalle immagini di base di AWS e dei partner APN.
2. Automatizza la gestione delle configurazioni. Applica e convalida in automatico le configurazioni sicure nelle risorse di calcolo utilizzando un servizio o uno strumento di gestione della configurazione.
   a. Gestione automatizzata della configurazione tramite AWS Config
   b. Gestione automatizzata del livello di sicurezza e conformità tramite AWS Security Hub CSPM

3. Automatizza applicazione delle patch o sostituzione delle istanze Amazon Elastic Compute Cloud (Amazon EC2). AWS Gestione patch di Systems Manager automatizza il processo di applicazione di patch alle istanze gestite con aggiornamenti correlati alla sicurezza e di altro tipo. Gestione patch consente di applicare patch sia per i sistemi operativi sia per le applicazioni
   a. AWS Systems Manager Patch Manager
4. Automatizza la scansione delle risorse di calcolo alla ricerca di vulnerabilità ed esposizioni comuni (CVE) e integra le soluzioni di scansione della sicurezza nella tua pipeline di compilazione.
   a. Amazon Inspector
   b. Scansione delle immagini ECR
5. Prendi in considerazione Amazon GuardDuty per il rilevamento automatico di malware e minacce al fine di proteggere le risorse di calcolo. GuardDuty può anche identificare potenziali problemi in caso di richiamo di una funzione AWS Lambda nel tuo ambiente AWS.
   a. Amazon GuardDuty
6. Prendi in considerazione le soluzioni dei partner AWS. AWS I partner offrono prodotti leader nel settore che sono equivalenti, identici o si integrano ai controlli esistenti negli ambienti on-premises. Questi prodotti integrano i servizi AWS esistenti per permettere di implementare un'architettura di sicurezza completa e un'esperienza più fluida nel cloud e negli ambienti on-premises.
   a. Sicurezza dell'infrastruttura

Risorse

Best practice correlate:

- SEC01-BP06 Implementazione automatizzata dei controlli di sicurezza standard

Documenti correlati:

- Get the full benefits of IMDSv2 and disable IMDSv1 across your AWS infrastructure

Video correlati:

- Security best practices for the Amazon EC2 instance metadata service

Protezione dei dati

Prima di progettare qualsiasi carico di lavoro, dovrebbero essere messe in atto pratiche fondamentali che influenzano la sicurezza. Ad esempio, la classificazione dei dati fornisce un modo per categorizzare i dati in base ai livelli di sensibilità mentre la crittografia protegge i dati rendendoli incomprensibili agli accessi non autorizzati. Questi metodi sono importanti perché supportano obiettivi quali la prevenzione di una gestione errata o la conformità agli obblighi normativi.

In AWS, è possibile utilizzare diversi approcci per la protezione dei dati. La seguente sezione descrive come utilizzare questi approcci.

Argomenti

Classificazione dei dati

La classificazione dei dati fornisce un modo per categorizzare i dati dell'organizzazione in base ai livelli di criticità e sensibilità, in modo da aiutarti a determinare i controlli di protezione e conservazione appropriati.

Best practice

SEC07-BP01 Comprendere lo schema di classificazione dei dati

Comprendi la classificazione dei dati elaborati dal tuo carico di lavoro, i requisiti di gestione, i processi aziendali associati, dove sono archiviati i dati e chi è il relativo proprietario. Lo schema di classificazione e gestione dei dati deve tenere conto dei requisiti legali e di conformità applicabili del carico di lavoro e dei controlli dei dati necessari. Comprendere i dati è il primo passo nel percorso della classificazione dei dati.

Risultato desiderato: comprensione e documentazione ottimali dei tipi di dati presenti nel carico di lavoro. Sono in atto controlli adeguati per proteggere i dati sensibili in base alla loro classificazione. Questi controlli regolano considerazioni quali chi è autorizzato ad accedere ai dati e per quale scopo, la posizione di archiviazione dei dati, qual è la policy di crittografia per tali dati e le modalità di gestione delle chiavi di crittografia, il ciclo di vita dei dati e i requisiti di conservazione, i processi di distruzione opportuni, i processi di backup e ripristino in atto, nonché la verifica degli accessi.

Anti-pattern comuni:

- Non si dispone di una policy formale di classificazione dei dati per definire i livelli di sensibilità dei dati e i relativi requisiti di gestione.
- Non si dispone di una corretta consapevolezza dei livelli di sensibilità dei dati all'interno del carico di lavoro e non si acquisiscono queste informazioni nella documentazione dell'architettura e delle operazioni.
- Mancata applicazione di controlli appropriati sui dati in base alla loro sensibilità e ai requisiti, come indicato nella relativa policy di classificazione e trattamento.
- Mancata indicazione di un feedback sui requisiti di classificazione e trattamento dei dati ai proprietari delle policy.

Vantaggi dell'adozione di questa best practice: eliminazione delle ambiguità circa la corretta gestione dei dati nell'ambito del carico di lavoro grazie a questa pratica. L'applicazione di una policy formale che definisca i livelli di sensibilità dei dati nella propria organizzazione e le relative protezioni richieste, può aiutare a rispettare le normative legali e altre attestazioni e certificazioni di sicurezza informatica. I proprietari dei carichi di lavoro possono avere la certezza di sapere dove sono archiviati i dati sensibili e quali controlli di protezione sono in atto. La loro acquisizione nella documentazione aiuta i nuovi membri del team a comprenderli meglio e a gestire i controlli nelle prime fasi del loro mandato. Queste pratiche possono anche aiutare a ridurre i costi, dimensionando in modo corretto i controlli per ogni tipo di dati.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Nella progettazione di un carico di lavoro, si può prendere in considerazione soluzioni per proteggere i dati sensibili in modo intuitivo. Ad esempio, in un'applicazione multi-tenant, è intuitivo considerare i dati di ciascun tenant come sensibili e mettere in atto protezioni in modo da vietare a un tenant l'accesso ai dati di un altro tenant. Allo stesso modo, è possibile progettare in modo intuitivo i

controlli di accesso in modo che solo gli amministratori possano modificare i dati, e che gli altri utenti abbiano solo accesso a livello di lettura o non dispongano di alcun accesso.

Definizione e acquisizione di questi livelli di sensibilità dei dati nelle policy, insieme ai relativi requisiti di protezione dei dati, consente di identificare in modo formale la residenza dei dati nel tuo carico di lavoro. È quindi possibile determinare se sono stati predisposti i controlli giusti, se è possibile verificare i controlli e quali sono le risposte adeguate in caso di gestione errata dei dati.

Per capire dove risiedono i dati sensibili all'interno del carico di lavoro, valuta la possibilità di utilizzare un catalogo dati. Un catalogo dati è un database che mappa i dati nell'organizzazione, con la relativa posizione, il livello di sensibilità e i controlli messi in atto per proteggerli. Valuta inoltre la possibilità di utilizzare i tag delle risorse, se disponibili. Ad esempio, puoi applicare un tag con una chiave di tag di `Classification` e un valore di tag di `PHI` per informazioni sanitarie protette (PHI) e un altro tag con una chiave di tag di `Sensitivity` e un valore di tag pari a `High`. È possibile usare servizi come AWS Config per monitorare tali risorse al fine di rilevare eventuali modifiche e inviare avvisi in caso di modifiche tali da renderle non conformi ai requisiti di protezione (come la modifica delle impostazioni di crittografia). È possibile acquisire la definizione standard delle chiavi tag e dei valori accettabili utilizzando le policy di tag, una funzionalità di AWS Organizations. Non è consigliabile che la chiave o il valore dei tag contenga dati privati o sensibili.

Passaggi dell'implementazione

1. Analizza lo schema di classificazione dei dati e i requisiti di protezione della tua organizzazione.
2. Identifica i tipi di dati sensibili elaborati dai tuoi carichi di lavoro.
3. Acquisisci i dati in un catalogo dedicato che offre una vista unica della posizione in cui risiedono i dati nell'organizzazione e del livello di sensibilità dei dati.
4. Prendi in considerazione l'utilizzo di tag a livello di risorse e dati, laddove disponibili, per etichettare i dati con il relativo livello di sensibilità e altri metadati operativi che possono aiutare nel monitoraggio e nella risposta agli incidenti.
   a. Le policy dei tag AWS Organizations consentono di applicare gli standard di etichettatura.

Risorse

Best practice correlate:

- SUS04-BP01 Implementazione di una policy di classificazione dei dati

Documenti correlati:

- Whitepaper sulla classificazione dei dati
- Best Practices for Tagging AWS Resources

Esempi correlati:

- AWS Organizations Tag Policy Syntax and Examples

Strumenti correlati

- Editor di tag AWS

SEC07-BP02 Applicazione di controlli di protezione dei dati in base alla loro sensibilità

Applica controlli di protezione dei dati che forniscano un livello di controllo adeguato a ciascuna classe di dati definita nella tua policy di classificazione. Questa pratica consente di proteggere i dati sensibili dall'accesso e dall'uso non autorizzati, preservandone al contempo disponibilità e utilizzo.

Risultato desiderato: presenza di una policy di classificazione che definisce i vari livelli di sensibilità dei dati nella tua organizzazione. Per ciascuno di questi livelli di sensibilità, disponi di linee guida chiare per servizi e luoghi di archiviazione e movimentazione approvati e per la loro configurazione richiesta. Implementi controlli per ciascun livello in base al livello di protezione richiesto e ai costi associati. Disponi di un sistema di monitoraggio e di avvisi per rilevare la presenza di dati in luoghi non autorizzati, l'elaborazione in ambienti non autorizzati, l'accesso da parte di soggetti non autorizzati o la configurazione di servizi correlati non conformi.

Anti-pattern comuni:

- Applicazione dello stesso livello di controlli di protezione su tutti i dati. Ciò può portare a un eccesso di controlli di sicurezza per i dati a bassa sensibilità o a una protezione insufficiente dei dati altamente sensibili.
- Mancato coinvolgimento delle parti interessate dei team di sicurezza, conformità e business nella definizione dei controlli sulla protezione dei dati.
- Si trascurano le spese generali e i costi operativi associati all'implementazione e al mantenimento dei controlli sulla protezione dei dati.

- Mancata effettuazione di revisioni periodiche del controllo della protezione dei dati per mantenere l'allineamento con le policy di classificazione.
- Assenza di un inventario completo delle posizioni in cui risiedono i dati a riposo e in transito.

Vantaggi dell'adozione di questa best practice: grazie all'allineamento dei controlli al livello di classificazione dei dati, l'organizzazione può investire in livelli di controllo più elevati, laddove necessario. Ciò può includere l'aumento delle risorse per la sicurezza, il monitoraggio, la misurazione, la correzione e la creazione di report. Se è opportuno disporre di meno controlli, è possibile migliorare l'accessibilità e la completezza dei dati per il personale, i clienti o gli utenti. Questo approccio offre alla tua organizzazione la massima flessibilità nell'utilizzo dei dati, pur rispettandone i requisiti di protezione.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

L'implementazione dei controlli di protezione dei dati in base ai loro livelli di sensibilità comporta diverse fasi fondamentali. In promo luogo, identifica i diversi livelli di sensibilità dei dati all'interno dell'architettura del tuo carico di lavoro (ad esempio, pubblico, interno, riservato e limitato) e valuta il luogo in cui memorizzi ed elabori questi dati. Quindi, definisci i limiti di isolamento dei dati in base al loro livello di sensibilità. Ti consigliamo di separare i dati in diversi Account AWS, utilizzando le policy di controllo dei servizi (SCP) per limitare servizi e azioni consentiti per ciascun livello di sensibilità dei dati. In questo modo, puoi creare forti limiti di isolamento e far rispettare il principio del privilegio minimo.

Una volta definiti i limiti di isolamento, implementa i controlli di protezione adeguati in base ai loro livelli di sensibilità. Consulta le best practice per la protezione dei dati a riposo e la protezione dei dati in transito in modo da implementare controlli pertinenti come la crittografia, i controlli di accesso e gli audit. Prendi in considerazione tecniche come la tokenizzazione o l'anonimizzazione per ridurre il livello di sensibilità dei tuoi dati. Semplifica l'applicazione di policy coerenti sui dati in tutta l'azienda con un sistema centralizzato per la tokenizzazione e la de-tokenizzazione.

Monitora e verifica in modo continuo l'efficacia dei controlli implementati. Rivedi e aggiorna con regolarità lo schema di classificazione dei dati, le valutazioni dei rischi e i controlli di protezione in base all'evoluzione del panorama di dati e minacce dell'organizzazione. Allinea i controlli di protezione dei dati implementati con normative, standard e requisiti legali pertinenti del settore. Inoltre, procedi alla sensibilizzazione e formazione sulla sicurezza per aiutare i dipendenti a

comprendere lo schema di classificazione dei dati e le loro responsabilità nella gestione e protezione dei dati sensibili.

Passaggi dell'implementazione

1. Identifica i livelli di classificazione e sensibilità dei dati all'interno del tuo carico di lavoro.
2. Definisci i limiti di isolamento per ciascun livello e determina una strategia di applicazione.
3. Valuta i controlli definiti che regolano accesso, crittografia, verifica, conservazione e altri aspetti richiesti dalla policy di classificazione dei dati.
4. Valuta le opzioni per ridurre il livello di sensibilità dei dati laddove appropriato, ad esempio utilizzando la tokenizzazione o l'anonimizzazione.
5. Verifica i tuoi controlli utilizzando test e monitoraggio automatici delle risorse configurate.

Risorse

Best practice correlate:

- PERF03-BP01 Uso di un archivio dati dedicato che supporta al meglio i requisiti di accesso e archiviazione dei dati
- COST04-BP05 Applicare policy di conservazione dei dati

Documenti correlati:

- Whitepaper sulla classificazione dei dati
- Best practice per la sicurezza, l'identità e la conformità
- Best practice di AWS KMS
- Encryption best practices and features for AWS services

Esempi correlati:

- Building a serverless tokenization solution to mask sensitive data
- How to use tokenization to improve data security and reduce audit scope

Strumenti correlati:

- AWS Key Management Service (AWS KMS)

- AWS CloudHSM
- AWS Organizations

SEC07-BP03 Automazione dell'identificazione e della classificazione

Automatizzare l'identificazione e la classificazione dei dati può aiutarti a implementare i controlli corretti. L'uso dell'automazione per aumentare la determinazione manuale riduce il rischio di errore umano e di esposizione.

Risultato desiderato: possibilità di verificare se sono in atto controlli adeguati in base alla policy di classificazione e gestione. Strumenti e servizi automatizzati ti aiutano a identificare e classificare il livello di sensibilità dei tuoi dati. L'automazione consente inoltre di monitorare in modo continuo gli ambienti in modo da rilevare e inviare avvisi se i dati vengono archiviati o gestiti in modo non autorizzato, così da poter intraprendere rapidamente azioni correttive.

Anti-pattern comuni:

- Affidarsi esclusivamente a processi manuali per l'identificazione e la classificazione dei dati, che possono essere soggetti a errori e richiedere tempi di lavoro lunghi. Questo può portare a una classificazione dei dati inefficiente e incoerente, soprattutto con l'aumento dei volumi di dati.
- Mancata predisposizione di meccanismi per tracciare e gestire le risorse di dati all'interno dell'organizzazione.
- Si trascura la necessità di un monitoraggio e di una classificazione continui dei dati durante i loro spostamenti e le loro trasformazioni all'interno dell'organizzazione.

Vantaggi dell'adozione di questa best practice: l'automazione di identificazione e classificazione dei dati può garantire un'applicazione più coerente e accurata dei controlli di protezione dei dati, così da ridurre il rischio di errore umano. L'automazione può inoltre fornire visibilità in merito ad accesso e movimento dei dati sensibili, così da rilevare le manipolazioni non autorizzate e intraprendere azioni correttive.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

Sebbene si ricorra spesso al giudizio umano per classificare i dati durante le fasi iniziali di progettazione di un carico di lavoro, è opportuno considerare la presenza di sistemi che automatizzino l'identificazione e la classificazione dei dati di test come controllo preventivo.

Ad esempio, agli sviluppatori può essere fornito uno strumento o un servizio per analizzare i dati rappresentativi e determinarne la sensibilità. All'interno di AWS, puoi caricare set di dati in Amazon S3 ed eseguirne la scansione mediante Amazon Macie, Amazon Comprehend o Amazon Comprehend Medical. Allo stesso modo, considera la scansione dei dati come parte dei test di unità e integrazione per individuare i casi in cui i dati sensibili non sono previsti. Gli avvisi sui dati sensibili in questa fase possono evidenziare le lacune nelle protezioni prima dell'implementazione in produzione. Altre funzionalità, come il rilevamento di dati sensibili in AWS Glue, Amazon SNS e Amazon CloudWatch, consentono inoltre di rilevare informazioni personali e intraprendere azioni di mitigazione. Per qualsiasi strumento o servizio automatizzato, esamina come definisce i dati sensibili e integralo con altre soluzioni umane o automatizzate per colmare eventuali lacune.

Come controllo investigativo, utilizza il monitoraggio continuo degli ambienti per rilevare l'eventuale archiviazione non conforme dei dati sensibili. In questo modo puoi rilevare situazioni come l'emissione di dati sensibili nei file di log o la loro copia in un ambiente di analisi dei dati senza un'adeguata de-identificazione o redazione. I dati archiviati in Amazon S3 possono essere costantemente monitorati per verificare la presenza di dati sensibili grazie ad Amazon Macie.

Passaggi dell'implementazione

1. Esamina lo schema di classificazione dei dati all'interno dell'organizzazione descritto in SEC07-BP01.
   a. Una volta compreso lo schema di classificazione dei dati dell'organizzazione, puoi stabilire processi accurati per l'identificazione e la classificazione automatica in linea con le policy aziendali.
2. Esegui una scansione iniziale degli ambienti per l'identificazione e la classificazione automatica.
   a. Una prima scansione completa dei dati può aiutare a capire la residenza dei dati sensibili nei tuoi ambienti. Qualora una scansione completa non sia inizialmente richiesta o non possa essere completata in anticipo a causa dei costi, valuta l'adeguatezza delle tecniche di campionamento per raggiungere i tuoi risultati. Ad esempio, Amazon Macie può essere configurato per eseguire un'ampia operazione automatizzata di rilevamento dei dati sensibili nei bucket S3. Questa funzionalità utilizza tecniche di campionamento per eseguire in modo efficiente in termini di costi un'analisi preliminare della residenza dei dati. È quindi possibile eseguire un'analisi più approfondita dei bucket S3 utilizzando un processo di rilevamento dei dati sensibili. Anche altri archivi di dati possono essere esportati su S3 per essere analizzati da Macie.
   b. Stabilisci il controllo degli accessi definito in SEC07-BP02 per le risorse di archiviazione dei dati identificate durante la scansione.

3. Configura scansioni continue dei tuoi ambienti.
    a. La capacità di rilevamento automatizzata dei dati sensibili di Macie consente di eseguire scansioni continue degli ambienti. I bucket S3 noti e autorizzati a memorizzare dati sensibili possono essere esclusi utilizzando un elenco di permessi in Macie.
4. Incorpora l'identificazione e la classificazione nei processi di compilazione e di test.
    a. Identifica gli strumenti utilizzabili dagli sviluppatori per analizzare i dati alla ricerca di sensibilità mentre i carichi di lavoro sono in fase di sviluppo. Utilizza questi strumenti come parte dei test di integrazione per avvisare quando i dati sensibili sono inaspettati e impedire un'ulteriore implementazione.
5. Implementa un sistema o un runbook per intervenire quando i dati sensibili vengono trovati in luoghi non autorizzati.
    a. Limita l'accesso ai dati utilizzando la correzione automatica. Ad esempio, puoi spostare i dati in un bucket S3 con accesso limitato o assegnare un tag all'oggetto se utilizzi il controllo degli accessi basato su attributi (ABAC). Inoltre, valuta la possibilità di mascherare i dati quando vengono rilevati.
    b. Avvisa i team addetti alla protezione dei dati e alla risposta agli incidenti affinché indaghino sulla causa principale dell'incidente. Ogni informazione appresa può aiutare a prevenire incidenti futuri.

Risorse

Documenti correlati:

- AWS Glue: Detect and process sensitive data
- Using managed data identifiers in Amazon SNS
- Amazon CloudWatch Logs: Help protect sensitive log data with masking

Esempi correlati:

- Enabling data classification for Amazon RDS database with Macie
- Detecting sensitive data in DynamoDB with Macie

Strumenti correlati:

- Amazon Macie

- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Glue

SEC07-BP04 Definizione della gestione del ciclo di vita dei dati scalabili

Esamina i requisiti del ciclo di vita dei dati in relazione ai loro diversi livelli di classificazione e gestione. Ciò può includere le modalità di gestione dei dati quando entrano per la prima volta nell'ambiente, il modo in cui i dati si trasformano e le regole per la loro distruzione. Prendi in considerazione fattori come periodi di conservazione, accesso, audit e monitoraggio della provenienza.

Risultato desiderato: classificazione dei dati il più vicino possibile al momento e all'ora dell'importazione. Quando la classificazione dei dati richiede il mascheramento, la tokenizzazione o altri processi che riducono il livello di sensibilità, si eseguono queste azioni il più vicino possibile al punto e al momento dell'importazione.

Elimini i dati in conformità con la policy in uso quando non è più opportuno conservarli, in base alla loro classificazione.

Anti-pattern comuni:

- Implementazione di un approccio unico alla gestione del ciclo di vita dei dati, senza considerare i diversi livelli di sensibilità e i requisiti di accesso.
- Valutazione della gestione del ciclo di vita solo dal punto di vista dei dati utilizzabili o dei dati di cui si esegue il backup, ma non di entrambi.
- Si presume che i dati immessi nel carico di lavoro siano validi, senza stabilirne il valore o la provenienza.
- Affidamento alla durabilità dei dati come sostituti dei backup e della protezione dei dati.
- Mantenimento dei dati oltre la loro utilità e il periodo di conservazione richiesto.

Vantaggi dell'adozione di questa best practice: una strategia di gestione del ciclo di vita dei dati ben definita e scalabile aiuta a mantenere la conformità normativa, migliora la sicurezza dei dati, ottimizza i costi di archiviazione e consente l'accesso e la condivisione efficienti dei dati mantenendo i controlli opportuni.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

I dati all'interno di un carico di lavoro sono spesso dinamici. La forma che assumono quando entrano nell'ambiente del carico di lavoro può essere diversa da quella che assumono quando vengono archiviati o utilizzati nella logica aziendale, nel reporting, nell'analisi o nel machine learning. Inoltre, il valore dei dati può cambiare nel tempo. Alcuni dati sono di natura temporale e perdono valore con il passare del tempo. Considera l'impatto di queste modifiche ai dati sulla valutazione del tuo schema di classificazione dei dati e dei controlli associati. Laddove possibile, utilizza un meccanismo automatizzato del ciclo di vita, come le policy del ciclo di vita di Amazon S3 e Amazon Data Lifecycle Manager, per configurare i processi di scadenza, archiviazione e conservazione dei dati. Per i dati memorizzati in DynamoDB, puoi utilizzare la funzionalità Time To Live (TTL) per definire un timestamp di scadenza elemento per elemento.

Distingui tra i dati disponibili per l'uso e quelli archiviati come backup. Prendi in considerazione l'utilizzo di AWS Backup per automatizzare il backup dei dati tra tutti i servizi AWS. Gli snapshot di Amazon EBS consentono di copiare un volume EBS e archiviarlo utilizzando le funzionalità di S3, tra cui ciclo di vita, protezione dei dati e accesso ai meccanismi di protezione. Due di questi meccanismi sono S3 Object Lock e AWS Backup Vault Lock, in grado di garantire sicurezza e controllo aggiuntivi ai backup. Gestisci una chiara separazione dei compiti e dell'accesso per i backup. Isola i backup a livello di account per mantenere la separazione dall'ambiente interessato durante un evento.

Un altro aspetto della gestione del ciclo di vita consiste nella registrazione della cronologia dei dati mentre avanzano nel carico di lavoro, chiamato tracciamento della provenienza dei dati. In questo modo hai la certezza di conoscere la provenienza dei dati, le trasformazioni effettuate, il proprietario o il processo che ha apportato le modifiche e la data. Questa cronologia è utile per la risoluzione dei problemi e le analisi in caso di potenziali eventi di sicurezza. Ad esempio, puoi creare log sui metadati relativi alle trasformazioni in una tabella Amazon DynamoDB. All'interno di un data lake, puoi conservare copie dei dati trasformati in diversi bucket S3 per ciascuna fase della pipeline di dati. Archivia le informazioni su schema e timestamp in un AWS Glue Data Catalog. Indipendentemente dalla tua soluzione, considera i requisiti degli utenti finali per determinare gli strumenti appropriati di cui hai bisogno per segnalare la provenienza dei tuoi dati. In questo modo potrai determinare come tracciare al meglio la tua provenienza.

Passaggi dell'implementazione

1. Analizza i tipi di dati, i livelli di sensibilità e i requisiti di accesso del carico di lavoro per classificare i dati e definire strategie di gestione del ciclo di vita appropriate.

2. Progetta e implementa policy di conservazione dei dati e processi di distruzione automatizzata in linea con i requisiti legali, normativi e organizzativi.
3. Stabilisci processi e automazione per il monitoraggio continuo, la verifica e l'adeguamento delle strategie, dei controlli e delle policy di gestione del ciclo di vita dei dati in base all'evoluzione dei requisiti del carico di lavoro e delle normative.
    a. Individua eventuali risorse per le quali non è attivata la gestione automatica del ciclo di vita con AWS Config.

Risorse

Best practice correlate:

- COST04-BP05 Applicare policy di conservazione dei dati
- SUS04-BP03 Utilizzo delle policy per gestire il ciclo di vita dei set di dati

Documenti correlati:

- Whitepaper sulla classificazione dei dati
- AWS Blueprint for Ransomware Defense
- DevOps Guidance: Improve traceability with data provenance tracking

Esempi correlati:

- How to protect sensitive data for its entire lifecycle in AWS
- Build data lineage for data lakes using AWS Glue, Amazon Neptune, and Spline

Strumenti correlati:

- AWS Backup
- Amazon Data Lifecycle Manager
- AWS Identity and Access Management Access Analyzer

Protezione dei dati a riposo

I dati a riposo rappresentano tutti i dati conservati nello storage non volatile per qualsiasi durata del carico di lavoro. Sono inclusi storage a blocchi, storage di oggetti, database, archivi, dispositivi IoT e qualsiasi altro supporto di storage su cui sono conservati i dati. La protezione dei dati a riposo riduce il rischio di accesso non autorizzato quando vengono implementati crittografia e controlli degli accessi adeguati.

La crittografia e la tokenizzazione sono due metodi di protezione dei dati importanti ma diversi.

La tokenizzazione è un processo che consente di definire un token per rappresentare un'informazione altrimenti sensibile (ad esempio, un token per rappresentare il numero di carta di credito di un cliente). Un token deve essere privo di significato e non deve derivare dai dati di cui sta effettuando la tokenizzazione; pertanto, un digest crittografico non è utilizzabile come token. Pianificando attentamente l'approccio alla tokenizzazione, puoi fornire una protezione aggiuntiva ai contenuti e assicurarti di soddisfare i requisiti di conformità. Ad esempio, puoi limitare l'ambito di conformità di un sistema di elaborazione delle carte di credito se utilizzi un token anziché un numero di carta di credito.

La crittografia è un sistema per trasformare i contenuti in modo da renderli illeggibili senza una chiave segreta necessaria per decrittare di nuovo i contenuti in testo normale. Sia la tokenizzazione che la crittografia possono essere utilizzate per mettere in sicurezza e proteggere le informazioni nel modo più adeguato. Inoltre, il mascheramento è una tecnica che consente di redigere una parte di dati fino a un punto in cui i dati rimanenti non sono considerati sensibili. Ad esempio, PCI-DSS consente di conservare le ultime quattro cifre di un numero di carta fuori dal limite dell'ambito di conformità per l'indicizzazione.

Audit dell'utilizzo delle chiavi di crittografia: assicurati di comprendere e controllare l'uso delle chiavi di crittografia per convalidare che i meccanismi di controllo degli accessi sulle chiavi siano implementati in modo appropriato. Ad esempio, qualsiasi servizio AWS che utilizza una chiave AWS KMS registra ogni utilizzo in AWS CloudTrail. Puoi quindi eseguire query AWS CloudTrail utilizzando uno strumento come gli Approfondimenti di Amazon CloudWatch Logs, per assicurarti che tutti gli utilizzi delle chiavi siano validi.

Best practice

- SEC08-BP01 Implementazione della gestione sicura delle chiavi
- SEC08-BP02 Applicazione della crittografia dei dati a riposo
- SEC08-BP03 Automatizzazione della protezione dei dati a riposo

- SEC08-BP04 Applicazione del controllo degli accessi

SEC08-BP01 Implementazione della gestione sicura delle chiavi

La gestione sicura delle chiavi include l'archiviazione, la rotazione, il controllo degli accessi e il monitoraggio del materiale relativo alla chiave necessario per proteggere i dati a riposo per il carico di lavoro.

Risultato desiderato: disponibilità di un meccanismo di gestione delle chiavi scalabile, ripetibile e automatizzato. Il meccanismo applica l'accesso con privilegio minimo al materiale relativo alle chiavi e offre il giusto equilibrio tra disponibilità, riservatezza e integrità delle chiavi. È possibile monitorare l'accesso alle chiavi e, se è necessaria la rotazione del materiale delle chiavi, tale operazione può essere eseguita tramite un processo automatizzato. L'accesso al materiale delle chiavi da parte di operatori umani non è consentito.

Anti-pattern comuni:

- Accesso umano a materiale relativo alla chiave non crittografato.
- Creazione di algoritmi crittografici personalizzati.
- Autorizzazioni di accesso al materiale relativo alla chiave di accesso troppo ampie.

Vantaggi dell'adozione di questa best practice: predisponendo un meccanismo di gestione delle chiavi sicuro per il tuo carico di lavoro, puoi contribuire a proteggere i contenuti dagli accessi non autorizzati. Inoltre, la crittografia dei dati potrebbe essere prevista da requisiti normativi per la tua organizzazione. Una soluzione efficace di gestione delle chiavi può fornire meccanismi tecnici finalizzati alla protezione del materiale relativo alle chiavi in linea con tali normative.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

La crittografia dei dati a riposo è un controllo di sicurezza fondamentale. Il carico di lavoro necessita di un meccanismo per archiviare e gestire in modo sicuro il materiale relativo alla chiave utilizzato per crittografare i dati a riposo.

AWS offre AWS Key Management Service (AWS KMS) per fornire uno spazio di archiviazione durevole, sicuro e ridondante per le chiavi AWS KMS. Molti servizi AWS si integrano con AWS KMS per supportare la crittografia dei dati. AWS KMS utilizza moduli di sicurezza hardware conformi allo

standard FIPS 140-3 di livello 3 per proteggere le chiavi. Non esiste un meccanismo per esportare le chiavi AWS KMS convertendole in testo semplice.

Nell'implementazione di carichi di lavoro mediante una strategia multi-account, le chiavi AWS KMS devono essere conservate nello stesso account del carico di lavoro che le utilizza. In questo modello distribuito la responsabilità della gestione delle chiavi AWS KMS spetta al tuo team. In altri casi d'uso, la tua organizzazione può scegliere di archiviare le chiavi AWS KMS in un account centralizzato. Questa struttura centralizzata richiede policy aggiuntive per consentire l'accesso multi-account richiesto affinché l'account del carico di lavoro possa accedere alle chiavi di accesso archiviate nell'account centralizzato, ma può essere più applicabile nei casi d'uso in cui una singola chiave è condivisa tra Account AWS multipli.

Indipendentemente dalla posizione in cui è archiviato il materiale relativo alla chiave, l'accesso alla chiave deve essere strettamente controllato mediante l'uso di policy della chiave e policy IAM. Le policy della chiave costituiscono la modalità principale per controllare l'accesso a una chiave AWS KMS. Inoltre, AWS KMS garantisce che le chiavi possano fornire l'accesso ai servizi AWS per crittografare e decrittografare i dati per tuo conto. Consulta le linee guida per il controllo degli accessi alle chiavi AWS KMS.

È necessario monitorare l'uso delle chiavi di crittografia per rilevare eventuali modelli di accesso insoliti. Le operazioni eseguite utilizzando chiavi gestite da AWS e chiavi gestite dal cliente archiviate in AWS KMS, possono essere registrate in AWS CloudTrail e devono essere riviste periodicamente. Presta particolare attenzione al monitoraggio degli eventi di eliminazione delle chiavi. Per ridurre le probabilità di distruzione accidentale o dolosa del materiale relativo alla chiave, gli eventi di eliminazione delle chiavi non hanno efficacia immediata. I tentativi di eliminazione delle chiavi in AWS KMS sono soggetti a un periodo di attesa, che per impostazione predefinita è di 30 giorni (con un minimo di 7 giorni), così da garantire agli amministratori il tempo di rivedere queste azioni e annullare la richiesta, se necessario.

La maggior parte dei servizi AWS utilizza AWS KMS secondo una modalità chiara per te: il tuo unico requisito è decidere se utilizzare una chiave gestita da AWS o dal cliente. Se il carico di lavoro richiede l'uso diretto di AWS KMS per crittografare o decrittografare i dati, occorre utilizzare la crittografia a busta per proteggere i tuoi dati. L'SDK di crittografia di AWS è in grado di fornire alle applicazioni primitive la crittografia lato client per implementare la crittografia a busta e integrarle con AWS KMS.

Passaggi dell'implementazione

1. Determina le opzioni di gestione delle chiavi adeguate (gestite da AWS o dal cliente) per la chiave.

   a. Per facilitare l'uso, AWS offre chiavi AWS di proprietà e gestite da AWS per la maggior parte dei servizi, fornendo funzionalità di crittografia a riposo senza la necessità di gestire il materiale o le policy della chiave.

   b. Quando utilizzi chiavi gestite dal cliente, prendi in considerazione il keystore predefinito per fornire il miglior equilibrio tra agilità, sicurezza, sovranità dei dati e disponibilità. Per altri casi d'uso può essere richiesto l'uso di archivi di chiavi personalizzati con AWS CloudHSM o l'archivio chiavi esterno.

2. Consulta l'elenco dei servizi che stai utilizzando per il tuo carico di lavoro per capire come AWS KMS si integra con il servizio. Ad esempio, le istanze EC2 possono utilizzare volumi EBS crittografati; verifica che anche gli snapshot Amazon EBS create da tali volumi siano crittografate utilizzando una chiave gestita dal cliente e mitigando la divulgazione accidentale di dati di snapshot non crittografati.

   a. How AWS services use AWS KMS

   b. Per informazioni dettagliate sulle opzioni di crittografia offerte da un servizio AWS, consulta l'argomento relativo alla crittografia dei dati a riposo nella guida per l'utente o nella guida per gli sviluppatori del servizio.

3. Implementa AWS KMS: AWS KMS semplifica la creazione e la gestione delle chiavi e controlla l'uso della crittografia in un'ampia gamma di servizi AWS e nelle tue applicazioni.

   a. Nozioni di base: AWS Key Management Service (AWS KMS)

   b. Consulta le best practices for access control to your AWS KMS keys.

4. Considera l'SDK di crittografia AWS: utilizza l'SDK di crittografia AWS con l'integrazione di AWS KMS quando la tua applicazione deve crittografare i dati lato client.

   a. SDK di crittografia AWS

5. Abilita IAM Access Analyzer per rivedere e inviare notifiche in automatico se esistono policy della chiave AWS KMS eccessivamente permissive.

   a. Valuta la possibilità di utilizzare controlli delle policy personalizzati per verificare che l'aggiornamento di una policy delle risorse non conceda l'accesso pubblico alle chiavi KMS.

6. Abilita Security Hub CSPM per ricevere notifiche in caso di policy della chiave configurate in modo errato, chiavi programmate per essere eliminate o chiavi senza la rotazione automatica abilitata.

7. Determina il livello di log appropriato per le tue chiavi AWS KMS. Poiché le chiamate a AWS KMS, inclusi gli eventi di sola lettura, vengono registrate, i log CloudTrail associati a AWS KMS possono diventare voluminosi.

a. Alcune organizzazioni preferiscono la segregazione dell'attività di log di AWS KMS in un percorso separato. Per maggiori dettagli, consulta la sezione Logging AWS KMS API calls with CloudTrail della guida per gli sviluppatori AWS KMS.

Risorse

Documenti correlati:

- AWS Key Management Service
- AWS cryptographic services and tools
- Protezione dei dati Amazon S3 tramite la crittografia
- Crittografia envelope
- Impegno per la sovranità digitale
- Demystifying AWS KMS key operations, bring your own key, custom key store, and ciphertext portability
- AWS Key Management Service Dettagli della crittografia di

Video correlati:

- How Encryption Works in AWS
- Securing Your Block Storage on AWS
- AWS data protection: Using locks, keys, signatures, and certificates

Esempi correlati:

- Implement advanced access control mechanisms using AWS KMS

SEC08-BP02 Applicazione della crittografia dei dati a riposo

Crittografando i dati privati a riposo è possibile mantenere la riservatezza e fornire un ulteriore livello di protezione contro la divulgazione o esfiltrazione involontaria dei dati. La crittografia protegge i dati in modo che non possano essere letti o consultati senza prima essere stati decrittografati. Effettua un inventario e un controllo dei dati non crittografati per mitigare i rischi associati all'esposizione dei dati.

Risultato desiderato: disponi di meccanismi che effettuano la crittografia dei dati privati per impostazione predefinita quando sono a riposo. Questi meccanismi aiutano a mantenere la riservatezza dei dati e forniscono un ulteriore livello di protezione contro la divulgazione o esfiltrazione involontaria dei dati. Mantieni un inventario dei dati non crittografati e comprendi i controlli in atto per proteggerli.

Anti-pattern comuni:

- Mancato utilizzo di configurazioni con crittografia predefinita.
- Accesso estremamente permissivo alle chiavi di decrittografia.
- Mancato monitoraggio dell'uso delle chiavi di crittografia e decrittografia.
- Memorizzazione di dati non crittografati.
- Utilizzo della stessa chiave di crittografia per tutti i dati, indipendentemente dall'uso, dal tipo e dalla classificazione dei dati stessi.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Mappa le chiavi di crittografia in base alle classificazioni dei dati all'interno dei carichi di lavoro. Questo approccio favorisce la protezione dei dati da accessi eccessivamente permissivi in caso di utilizzo di una sola chiave di crittografia o di un numero molto ridotto di chiavi di crittografia (vedi SEC07-BP01 Comprendere lo schema di classificazione dei dati).

AWS Key Management Service (AWS KMS) si integra con molti servizi AWS per semplificare la crittografia dei dati a riposo. Ad esempio, in Amazon Elastic Compute Cloud (Amazon EC2) puoi impostare la crittografia predefinita sugli account in modo che i nuovi volumi EBS vengano crittografati in automatico. Quando utilizzi AWS KMS, devi considerare il livello di restrizione dei dati. Le chiavi AWS KMS predefinite e controllate dal servizio sono gestite e utilizzate da AWS per tuo conto. Per i dati sensibili che richiedono un accesso granulare alla chiave di crittografia sottostante, è opportuno considerare le chiavi gestite dal cliente (CMK). L'utente ha il pieno controllo sulle CMK, anche per quanto riguarda la rotazione e la gestione degli accessi attraverso l'uso di policy sulla chiave.

Inoltre, servizi come Amazon Simple Storage Service (Amazon S3) effettuano ora la crittografia di tutti i nuovi oggetti per impostazione predefinita. Questa implementazione offre una maggiore sicurezza senza alcun impatto sulle prestazioni.

Altri servizi, ad esempio Amazon Elastic Compute Cloud (Amazon EC2) o Amazon Elastic File System (Amazon EFS), supportano impostazioni per la crittografia predefinita. Puoi utilizzare anche Regole di AWS Config per verificare in automatico che sia in uso la crittografia per i volumi Amazon Elastic Block Store (Amazon EBS), le istanze Amazon Relational Database Service (Amazon RDS), i bucket Amazon S3 e altri servizi all'interno della tua organizzazione.

AWS offre anche soluzioni per la crittografia lato client, consentendo di crittografare i dati prima di caricarli nel cloud. AWS Encryption SDK offre un modo per la crittografia dei dati mediante la crittografia a busta. L'utente fornisce la chiave di wrapping e AWS Encryption SDK genera una chiave dati unica per ogni oggetto di dati che crittografa. Prendi in considerazione AWS CloudHSM se hai bisogno di un modulo di sicurezza hardware (HSM) gestito single-tenant. AWS CloudHSM consente di generare, importare e gestire le chiavi crittografiche su un HSM convalidato FIPS 140-2 di livello 3. Alcuni casi d'uso di AWS CloudHSM includono la protezione delle chiavi private per il rilascio di un'autorità di certificazione (CA) e l'abilitazione della crittografia dei dati trasparente (TDE) per i database Oracle. Il client SDK AWS CloudHSM fornisce un software che consente di crittografare i dati sul lato client utilizzando le chiavi memorizzate all'interno di AWS CloudHSM prima di caricare i dati in AWS. La crittografia lato client Amazon DynamoDB consente inoltre di crittografare e firmare gli elementi prima del caricamento in una tabella DynamoDB.

Passaggi dell'implementazione

- Configura la crittografia predefinita per nuovi volumi Amazon EBS: specifica che desideri che tutti i volumi Amazon EBS appena creati vengano creati in forma crittografata, con la possibilità di utilizzare la chiave predefinita fornita da AWS oppure una chiave creata da te.
- Configura Amazon Machine Image (AMI) crittografate: copiando un'AMI esistente con crittografia abilitata, verrà eseguita la crittografia automatica di volumi root e snapshot.
- Configura la crittografia Amazon RDS: configura la crittografia per cluster e snapshot del database Amazon RDS a riposo abilitando l'opzione di crittografia.
- Crea e configura chiavi AWS KMS con policy che limitano l'accesso ai principali opportuni per ciascuna classificazione dei dati: ad esempio, crea una chiave AWS KMS per la crittografia dei dati di produzione e una chiave diversa per quella dei dati di sviluppo o di test. Puoi anche fornire l'accesso alle chiavi ad altri Account AWS. Considera la possibilità di predisporre account diversi per gli ambienti di sviluppo e di produzione. Qualora il tuo ambiente di produzione richieda la decodifica degli artefatti nell'account di sviluppo, puoi modificare la policy CMK utilizzata in modo da crittografare gli artefatti di sviluppo per consentire all'account di produzione di decrittografare tali artefatti. L'ambiente di produzione può quindi importare i dati decrittografati per utilizzarli nella produzione.

- Configura la crittografia nei servizi AWS aggiuntivi: per gli altri servizi AWS che utilizzi, consulta la documentazione di sicurezza relativa al servizio interessato per determinare le opzioni di crittografia del servizio.

Risorse

Documenti correlati:

- AWS Crypto Tools
- AWS Encryption SDK
- AWS KMS Cryptographic Details Whitepaper
- AWS Key Management Service
- AWS cryptographic services and tools
- Amazon EBS Encryption
- Default encryption for Amazon EBS volumes
- Encrypting Amazon RDS Resources
- Come si attiva la crittografia predefinita per un bucket Amazon S3?
- Protezione dei dati Amazon S3 tramite la crittografia

Video correlati:

- How Encryption Works in AWS
- Securing Your Block Storage on AWS

SEC08-BP03 Automatizzazione della protezione dei dati a riposo

Usa l'automazione per convalidare e applicare i controlli dei dati a riposo. Usa la scansione automatica per rilevare le configurazioni errate delle soluzioni di archiviazione di dati ed esegui le correzioni attraverso la risposta programmatica automatica, ove possibile. Incorpora l'automazione nei tuoi processi CI/CD per rilevare le configurazioni errate dell'archiviazione di dati prima che vengano implementate in produzione.

Risultato desiderato: scansione e monitoraggio da parte di sistemi automatizzati delle posizioni di archiviazione di dati per individuare configurazioni errate dei controlli, accessi non autorizzati e usi imprevisti. Il rilevamento delle posizioni di archiviazione non configurate avvia correzioni

automatiche. I processi automatizzati creano backup dei dati e archiviano copie immutabili al di fuori dell'ambiente originale.

Anti-pattern comuni:

- Mancata tenuta in considerazione delle opzioni per abilitare la crittografia dalle impostazioni predefinite, ove supportate.
- Mancata tenuta in considerazione degli eventi di sicurezza, oltre a quelli operativi, quando si formula una strategia di backup e ripristino automatizzata.
- Mancata applicazione delle impostazioni di accesso pubblico per i servizi di archiviazione.
- Assenza di monitoraggio e audit dei controlli per proteggere i dati a riposo.

Vantaggi dell'adozione di questa best practice: prevenzione grazie all'automazione del rischio di configurazioni errate delle posizioni di archiviazione di dati e dell'ingresso di configurazioni errate negli ambienti di produzione. Questa best practice aiuta anche a rilevare e correggere eventuali configurazioni errate.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

L'automazione è un tema ricorrente in tutte le pratiche per la protezione dei dati a riposo. SEC01-BP06 Implementazione automatizzata dei controlli di sicurezza standard illustra come acquisire la configurazione delle risorse utilizzando modelli di infrastructure as code (IaC), ad esempio con AWS CloudFormation. Questi modelli sono vincolati a un sistema di controllo della versione e consentono di distribuire risorse su AWS tramite una pipeline CI/CD. Queste tecniche si applicano anche all'automazione della configurazione delle soluzioni di archiviazione di dati, come le impostazioni di crittografia sui bucket Amazon S3.

Puoi controllare le impostazioni che definisci nei tuoi modelli IaC per eventuali configurazioni errate nelle pipeline CI/CD utilizzando le regole in AWS CloudFormation Guard. Puoi monitorare impostazioni non ancora disponibili in CloudFormation o in altri strumenti IaC per evitare configurazioni errate con AWS Config. È possibile correggere in automatico gli avvisi generati da Config per configurazioni errate, come illustrato in SEC04-BP04 Avvio della riparazione delle risorse non conformi.

L'utilizzo dell'automazione come parte della strategia di gestione delle autorizzazioni è anche parte integrante delle protezioni automatizzate dei dati. SEC03-BP02 Concessione dell'accesso

con privilegio minimo e SEC03-BP04 Riduzione delle autorizzazioni in modo continuo illustrano la configurazione delle policy di accesso con privilegio minimo monitorate di continuo da AWS Identity and Access Management Access Analyzer per generare esiti quando è possibile ridurre le autorizzazioni. Oltre all'automazione per il monitoraggio delle autorizzazioni, puoi configurare Amazon GuardDuty in modo da rilevare comportamenti anomali di accesso ai dati per i tuoi volumi EBS (tramite un'istanza EC2), bucket S3 e i database di Amazon Relational Database Service.

L'automazione svolge rileva inoltre i casi di archiviazione di dati sensibili in luoghi non autorizzati. SEC07-BP03 Automazione dell'identificazione e della classificazione illustra in che modo Amazon Macie può monitorare i bucket S3 alla ricerca di dati sensibili imprevisti e generare avvisi in grado di avviare una risposta automatica.

Segui le pratiche di REL09 In che modo eseguire il backup dei dati? per sviluppare una strategia automatizzata di backup e ripristino dei dati. Il backup e il ripristino dei dati sono importanti tanto per il ripristino da eventi di sicurezza quanto per gli eventi operativi.

Passaggi dell'implementazione

1. Acquisisci la configurazione dell'archiviazione di dati nei modelli IaC. Utilizza i controlli automatizzati nelle pipeline CI/CD per rilevare configurazioni errate.
   a. Puoi utilizzare CloudFormation per i modelli IaC e CloudFormation Guard per verificare la presenza di errori di configurazione nei modelli.
   b. Utilizza AWS Config per eseguire le regole in modalità di valutazione proattiva. Utilizza questa impostazione per verificare la conformità di una risorsa come passaggio della pipeline CI/CD prima di crearla.
2. Monitora le risorse per individuare eventuali configurazioni errate dell'archiviazione di dati.
   a. Imposta AWS Config in modo che monitori le risorse di archiviazione di dati al fine di rilevare eventuali modifiche nelle configurazioni di controllo e generare avvisi per richiamare correzioni in caso di rilevamento di una configurazione errata.
   b. Consulta SEC04-BP04 Avvio della riparazione delle risorse non conformi per ulteriori indicazioni sulle correzioni automatiche.
3. Monitora e riduci in modo continuo le autorizzazioni di accesso ai dati tramite l'automazione.
   a. È possibile eseguire IAM Access Analyzer in modo continuo così da generare avvisi in caso di potenziale riduzione delle autorizzazioni.
4. Monitora e avvisa in caso di comportamenti anomali di accesso ai dati.

   a. GuardDuty analizza sia le firme note delle minacce sia le deviazioni dai comportamenti di accesso di base per le risorse di archiviazione di dati, come volumi EBS, bucket S3 e database RDS.

5. Monitora e invia avvisi sui dati sensibili archiviati in luoghi inaspettati.
   a. Usa Amazon Macie per una scansione continua dei tuoi bucket S3 alla ricerca di dati sensibili.
6. Automatizza i backup sicuri e crittografati dei tuoi dati.
   a. AWS Backup è un servizio gestito che permette di creare backup di varie origini dati su AWS. Elastic Disaster Recovery ti consente di copiare carichi di lavoro completi del server e mantenere una protezione continua dei dati con un obiettivo del punto di ripristino (RPO) misurato in secondi. È possibile configurare entrambi i servizi in modo che lavorino all'unisono per automatizzare la creazione di backup dei dati e la loro copia in posizioni di failover. Questo può aiutare a mantenere i dati disponibili in caso di eventi operativi o di sicurezza.

Risorse

Best practice correlate:

- SEC01-BP06 Implementazione automatizzata dei controlli di sicurezza standard
- SEC03-BP02 Concessione dell'accesso con privilegio minimo
- SEC03-BP04 Riduzione delle autorizzazioni in modo continuo
- SEC04-BP04 Avvio della riparazione delle risorse non conformi
- SEC07-BP03 Automazione dell'identificazione e della classificazione
- REL09-BP02 Protezione e crittografia dei backup
- REL09-BP03 Esecuzione del backup dei dati in automatico

Documenti correlati:

- AWS Prescriptive Guidance: Automatically encrypt existing and new Amazon EBS volumes
- Ransomware Risk Management on AWS Using the NIST Cyber Security Framework (CSF)

Esempi correlati:

- How to use AWS Config proactive rules and AWS CloudFormation Hooks to prevent creation of noncompliant cloud resources

- Automate and centrally manage data protection for Amazon S3 with AWS Backup
- AWS re:Invent 2023 - Implement proactive data protection using Amazon EBS snapshots
- AWS re:Invent 2022 - Build and automate for resilience with modern data protection

Strumenti correlati:

- AWS CloudFormation Guard
- AWS CloudFormation Guard Rules Registry
- IAM Access Analyzer
- Amazon Macie
- AWS Backup
- Elastic Disaster Recovery

SEC08-BP04 Applicazione del controllo degli accessi

Per proteggere i dati a riposo, applica il controllo degli accessi utilizzando meccanismi come l'isolamento e il controllo delle versioni. Applica i controlli in base al privilegio minimo e all'accesso condizionale. Impedisci che venga consentito l'accesso pubblico ai dati.

Risultato desiderato: puoi verificare che l'accesso ai dati sia consentito solo agli utenti autorizzati, in base alle necessità. La protezione dei dati è assicurata da backup regolari e dal controllo delle versioni, per evitare che la modifica dei dati o la loro eliminazione intenzionale o non voluta. L'isolamento dei dati critici dagli altri dati ne protegge la riservatezza e l'integrità.

Anti-pattern comuni:

- Archiviazione dei dati con requisiti di sensibilità o classificazione diversi.
- Utilizzo di autorizzazioni troppo permissive sulle chiavi di decrittografia.
- Classificazione impropria dei dati.
- Nessun mantenimento di backup dettagliati dei dati importanti.
- Accesso persistente ai dati di produzione.
- Nessun audit dell'accesso ai dati o revisione periodica delle autorizzazioni.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

La protezione dei dati a riposo è importante per mantenere l'integrità, la riservatezza e la conformità dei dati ai requisiti normativi. Per ottenere tale risultato puoi implementare più controlli, inclusi controllo degli accessi, isolamento, accesso condizionale e controllo delle versioni.

Puoi applicare il controllo degli accessi con il principio del privilegio minimo, che fornisce solo le autorizzazioni necessarie agli utenti e ai servizi per eseguire le varie attività. È incluso l'accesso alle chiavi di crittografia. Rivedi le policy AWS Key Management Service (AWS KMS) per verificare che il livello di accesso concesso sia appropriato e che si applichino le condizioni pertinenti.

Puoi separare i dati in base a diversi livelli di classificazione utilizzando Account AWS distinti per ogni livello e gestire tali account con AWS Organizations. Tale isolamento può aiutare a prevenire l'accesso non autorizzato e a ridurre al minimo il rischio di esposizione dei dati.

Rivedi periodicamente il livello di accesso concesso nelle policy dei bucket Amazon S3. Evita di utilizzare bucket leggibili o scrivibili pubblicamente a meno che ciò non sia assolutamente necessario. Valuta la possibilità di utilizzare AWS Config per rilevare i bucket disponibili pubblicamente e Amazon CloudFront per distribuire i contenuti da Amazon S3. Verifica che i bucket che non devono consentire l'accesso pubblico siano configurati correttamente a tale scopo.

Implementa meccanismi di controllo delle versioni e Object Lock per i dati critici archiviati in Amazon S3. Il controllo delle versioni di Amazon S3 preserva le versioni precedenti degli oggetti per recuperare i dati in caso di cancellazioni o sovrascritture accidentali. Amazon S3 Object Lock fornisce un controllo degli accessi obbligatorio per gli oggetti, che impedisce che questi ultimi vengano eliminati o sovrascritti, anche dall'utente root, fino alla scadenza del blocco. Inoltre, Amazon Glacier Vault Lock offre una funzionalità simile per gli archivi memorizzati in Amazon Glacier.

Passaggi dell'implementazione

1. Implementa il controllo degli accessi con il principio del privilegio minimo:
   - Verifica le autorizzazioni di accesso concesse a utenti e servizi e verifica che dispongano solo delle autorizzazioni necessarie per svolgere le rispettive attività.
   - Verifica l'accesso alle chiavi di crittografia controllando le policy AWS Key Management Service (AWS KMS).
2. Separa i dati in base a diversi livelli di classificazione:
   - Utilizza Account AWS distinti per ogni livello di classificazione dei dati.
   - Gestisci questi account utilizzando AWS Organizations.

3. Verifica le autorizzazioni per bucket e oggetti Amazon S3:
    - Rivedi periodicamente il livello di accesso concesso nelle policy dei bucket Amazon S3.
    - Evita di utilizzare bucket leggibili o scrivibili pubblicamente a meno che ciò non sia assolutamente necessario.
    - Valuta la possibilità di utilizzare AWS Config per rilevare i bucket pubblicamente disponibili.
    - Utilizza Amazon CloudFront per distribuire contenuti da Amazon S3.
    - Verifica che i bucket che non devono consentire l'accesso pubblico siano configurati correttamente a tale scopo.
    - Puoi applicare lo stesso processo di revisione per i database e qualsiasi altra origine dati che utilizzi l'autenticazione IAM, come SQS o datastore di terze parti.
4. Utilizza il Sistema di analisi degli accessi AWS IAM:
    - Puoi configurare AWS IAM Access Analyzer per analizzare i bucket Amazon S3 e generare esiti quando una policy S3 concede l'accesso a un'entità esterna.
5. Implementa meccanismi di controllo delle versioni e Object Lock:
    - Utilizza il controllo delle versioni di Amazon S3 per preservare le versioni precedenti degli oggetti, consentendo così il ripristino in caso di cancellazioni o sovrascritture accidentali.
    - Utilizza Amazon S3 Object Lock per fornire un controllo degli accessi obbligatorio per gli oggetti, che impedisce che questi ultimi vengano eliminati o sovrascritti, anche dall'utente root, fino alla scadenza del blocco.
    - Utilizza Amazon Glacier Vault Lock per gli archivi in Amazon Glacier.
6. Utilizza l'Inventario Amazon S3:
    - Puoi utilizzare l'Inventario Amazon S3 per eseguire audit e segnalare lo stato di replica e crittografia dei tuoi oggetti S3.
7. Verifica le autorizzazioni di condivisione di Amazon EBS e AMI:
    - Esamina le tue autorizzazioni di condivisione di Amazon EBS e AMI per verificare che le immagini e i volumi non vengano condivisi con Account AWS esterni al tuo carico di lavoro.
8. Rivedi periodicamente le condivisioni di AWS Resource Access Manager:
    - Puoi utilizzare AWS Resource Access Manager per condividere risorse come le policy AWS Network Firewall, le regole del risolutore Amazon Route 53 e le sottoreti all'interno dei tuoi Amazon VPC.
    - Sottoponi regolarmente ad audit le risorse condivise e interrompi la condivisione delle risorse che non devono più essere condivise.

Risorse

Best practice correlate:

- SEC03-BP01 Definizione dei requisiti di accesso
- SEC03-BP02 Concessione dell'accesso con privilegio minimo

Documenti correlati:

- AWS KMS Cryptographic Details Whitepaper
- Introduzione alla gestione delle autorizzazioni di accesso alle risorse di Amazon S
- Panoramica della gestione dell'accesso alle risorse AWS KMS
- Regole di AWS Config
- Amazon S3 + Amazon CloudFront: A Match Made in the Cloud
- Utilizzo del controllo delle versioni
- Blocco degli oggetti mediante Object Lock di Amazon S
- Sharing an Amazon EBS Snapshot
- AMI condivise
- Ospitare un'applicazione a pagina singola su Amazon S3
- AWS Global Condition Keys
- Building a Data Perimeter on AWS

Video correlati:

- Securing Your Block Storage on AWS

Protezione dei dati in transito

I dati in transito sono tutti i dati inviati da un sistema a un altro. Ciò include la comunicazione tra le risorse all'interno del carico di lavoro e la comunicazione tra altri servizi e gli utenti finali. Fornendo il livello di protezione appropriato per i dati in transito, proteggi la riservatezza e l'integrità dei dati del carico di lavoro.

Proteggi i dati tra VPC o sedi on-premises: AWS PrivateLink ti permette di creare una connessione di rete sicura e privata tra Amazon Virtual Private Cloud (Amazon VPC) o connettività on-premises

verso i servizi ospitati in AWS. Puoi accedere ai servizi AWS, ai servizi di terze parti e ai servizi in altri Account AWS, come se fossero sulla tua rete privata. Con AWS PrivateLink puoi accedere ai servizi negli account con sovrapposizioni IP CIDR, senza necessità di un gateway Internet o di un NAT. Non è richiesta la configurazione di regole del firewall, di definizioni di percorso o di tabelle di routing. Il traffico resta sul backbone di Amazon e non attraversa internet, per cui i tuoi dati sono protetti. Puoi garantire la conformità a normative specifiche di settore, come HIPAA ed EU/US Privacy Shield. AWS PrivateLink collabora in modo fluido con soluzioni di terze parti per creare una rete globale semplificata, consentendoti di accelerare la migrazione al cloud e di sfruttare i servizi AWS disponibili.

Best practice

- SEC09-BP01 Implementazione della gestione sicura delle chiavi e dei certificati
- SEC09-BP02 Applicazione della crittografia dei dati in transito
- SEC09-BP03 Autenticazione delle comunicazioni di rete

SEC09-BP01 Implementazione della gestione sicura delle chiavi e dei certificati

I certificati Transport Layer Security (TLS) vengono utilizzati per proteggere le comunicazioni di rete e stabilire l'identità di siti Web, risorse e carichi di lavoro su Internet, nonché sulle reti private.

Risultato desiderato: un sistema di gestione dei certificati sicuro in grado di fornire, implementare, archiviare e rinnovare i certificati in un'infrastruttura a chiave pubblica (PKI). Un meccanismo sicuro di gestione delle chiavi e dei certificati impedisce la divulgazione del materiale relativo alle chiavi private dei certificati e rinnova in automatico il certificato su base periodica. Si integra inoltre con altri servizi per fornire comunicazioni di rete e identità sicure per le risorse delle macchine all'interno del carico di lavoro. Il materiale relativo alla chiave non dovrebbe mai essere accessibile alle identità umane.

Anti-pattern comuni:

- Esecuzione di passaggi manuali durante i processi di distribuzione, implementazione o rinnovo dei certificati.
- Attenzione insufficiente alla gerarchia delle autorità di certificazione (CA) durante la progettazione di una CA privata.
- Utilizzo di certificati autofirmati per risorse pubbliche.

Vantaggi dell'adozione di questa best practice:

- Semplificazione della gestione dei certificati attraverso la distribuzione, l'implementazione e il rinnovo automatizzati
- Incoraggiamento dell'utilizzo della crittografia dei dati in transito con l'utilizzo di certificati TLS
- Maggiore sicurezza e verificabilità delle operazioni di certificazione intraprese dall'autorità di certificazione
- Organizzazione delle mansioni di gestione ai diversi livelli della gerarchia della CA

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

I carichi di lavoro moderni fanno ampio uso di comunicazioni di rete crittografate utilizzando protocolli PKI come TLS. La gestione dei certificati PKI può essere complessa, ma la fornitura, la distribuzione, l'implementazione e il rinnovo automatizzati dei certificati possono ridurre gli ostacoli associati alla loro gestione.

AWS fornisce due servizi per la gestione dei certificati PKI generici: AWS Certificate Manager e AWS Autorità di certificazione privata (AWS Private CA). ACM è il servizio principale utilizzato dai clienti per fornire, gestire e implementare certificati da utilizzare in carichi di lavoro pubblici e privati AWS. ACM rilascia certificati privati mediante AWS Private CA e si integra con diversi altri servizi AWS gestiti per mettere a disposizione certificati TLS sicuri per i carichi di lavoro. ACM può rilasciare anche certificati pubblicamente attendibili da Amazon Trust Services. I certificati pubblici rilasciati da ACM possono essere utilizzati per i carichi di lavoro pubblici, poiché i browser e i sistemi operativi moderni considerano tali certificati attendibili per impostazione predefinita.

AWS Private CA consente di stabilire la propria autorità di certificazione principale o subordinata e di emettere certificati TLS tramite un'API. È possibile utilizzare questo tipo di certificati in scenari in cui si mantengono il controllo e la gestione della catena di attendibilità sul lato client della connessione TLS. Oltre ai casi d'uso TLS, AWS Private CA consente di emettere certificati per i pod Kubernetes, gli attestati dei prodotti dei dispositivi Matter, la firma del codice e altri casi d'uso che prevedono un modello personalizzato. Puoi anche usare IAM Roles Anywhere per fornire credenziali IAM temporanee ai carichi di lavoro on-premises ai quali sono stati assegnati certificati X.509 firmati dalla tua CA privata.

Oltre a ACM e AWS Private CA, AWS IoT Core fornisce supporto specializzato per il provisioning, la gestione e l'implementazione di certificati PKI su dispositivi IoT. AWS IoT Core offre meccanismi specializzati per l'onboarding dei dispositivi IoT nella tua infrastruttura chiave pubblica su larga scala.

Alcuni servizi AWS, come Gateway Amazon API ed Elastic Load Balancing, offrono funzionalità proprie per l'utilizzo dei certificati per proteggere le connessioni delle applicazioni. Ad esempio, sia Gateway API che Application Load Balancer (ALB) supportano il protocollo mTLS utilizzando certificati client creati ed esportati utilizzando la Console di gestione AWS, la CLI o le API.

Considerazioni sulla creazione di una gerarchia CA privata

Quando occorre stabilire una CA privata, è importante prestare particolare attenzione a progettare in modo corretto la gerarchia della CA fin dall'inizio. Nella creazione di una gerarchia CA privata, è consigliabile distribuire ciascun livello della gerarchia CA su Account AWS separati. Questo passaggio intenzionale riduce l'estensione di ogni livello della gerarchia della CA, semplificando l'individuazione delle anomalie nei dati di log di CloudTrail e riducendo l'ambito di accesso o l'impatto in caso di accesso non autorizzato a uno degli account. La CA principale deve risiedere in un account separato e va utilizzata solo per l'emissione di uno o più certificati CA intermedi.

Quindi, crea una o più CA intermedie in account separati dall'account della CA principale per emettere certificati per utenti finali, dispositivi o altri carichi di lavoro. Infine, emetti certificati della tua CA principale a uso delle CA intermedie, che a loro volta emetteranno certificati per gli utenti finali o i dispositivi. Per ulteriori informazioni sulla pianificazione dell'implementazione della CA e sulla progettazione della gerarchia delle CA, inclusa la pianificazione della resilienza, la replica tra regioni, la condivisione delle CA all'interno dell'organizzazione e altro ancora, consulta Planning your AWS Private CA deployment.

Passaggi dell'implementazione

1. Determina i servizi AWS pertinenti richiesti per il tuo caso d'uso:
    - Molti casi d'uso possono sfruttare l'infrastruttura a chiave pubblica AWS esistente utilizzando AWS Certificate Manager. ACM consente di implementare certificati TLS per server Web, bilanciatori del carico o altri usi per certificati pubblicamente affidabili.
    - Prendi in considerazione AWS Private CA se occorre stabilire una gerarchia di autorità di certificazione privata o accedere a certificati esportabili. ACM può quindi essere utilizzato per emettere molti tipi di certificati di entità finale utilizzando AWS Private CA.
    - Per i casi d'uso in cui i certificati devono essere forniti su larga scala per dispositivi Internet delle cose (IoT) integrati, prendi in considerazione l'uso di AWS IoT Core.
    - Valuta la possibilità di utilizzare la funzionalità mTLS nativa in servizi come Gateway Amazon API o Application Load Balancer.
2. Implementa il rinnovo automatico dei certificati quando possibile:

- Usa il rinnovo gestito da ACM per i certificati emessi da ACM insieme ai servizi AWS gestiti integrati.

3. Stabilisci la creazione di log e audit trail:
   - Abilita i log CloudTrail per tenere traccia degli accessi agli account che detengono le autorità di certificazione. Prendi in considerazione la possibilità di configurare la convalida dell'integrità dei file di log in CloudTrail per verificarne l'autenticità dei dati.
   - Crea e rivedi a cadenza periodica report di audit che elencano i certificati emessi o revocati dalla tua CA privata. Questi report possono essere esportati in un bucket S3.
   - Quando si implementa una CA privata, è inoltre necessario creare un bucket S3 per archiviare l'elenco di revoche dei certificati (CRL). Per indicazioni sulla configurazione di questo bucket S3 in base ai requisiti del carico di lavoro, consulta Planning a certificate revocation list (CRL).

Risorse

Best practice correlate:

- SEC02-BP02 Utilizzo di credenziali temporanee
- SEC08-BP01 Implementazione della gestione sicura delle chiavi
- SEC09-BP03 Autenticazione delle comunicazioni di rete

Documenti correlati:

- How to host and manage an entire private certificate infrastructure in AWS
- How to secure an enterprise scale ACM Private CA hierarchy for automotive and manufacturing
- Private CA best practices
- How to use AWS RAM to share your ACM Private CA cross-account

Video correlati:

- Activating AWS Certificate Manager Private CA (workshop)

Esempi correlati:

- Private CA workshop
- IOT Device Management Workshop (compreso il provisioning dei dispositivi)

Strumenti correlati:

- Plugin to Kubernetes cert-manager to use AWS Private CA

SEC09-BP02 Applicazione della crittografia dei dati in transito

Applica i requisiti di crittografia definiti in base alle policy, agli obblighi normativi e agli standard dell'organizzazione per contribuire a soddisfare i requisiti organizzativi, legali e di conformità. Utilizza solo protocolli con crittografia quando trasmetti dati sensibili al di fuori del tuo cloud privato virtuale (VPC). La crittografia aiuta a mantenere la riservatezza dei dati anche quando questi transitano su reti non affidabili.

Risultato desiderato: il traffico di rete tra le tue risorse e Internet viene crittografato per evitare l'accesso non autorizzato ai dati. Il traffico di rete nell'ambiente AWS interno viene crittografato in base ai tuoi requisiti di sicurezza. I dati in transito vengono crittografati mediante protocolli TLS sicuri e suite di crittografia.

Anti-pattern comuni:

- Utilizzo di versioni obsolete di SSL, TLS e componenti della suite di crittografia (ad esempio, SSL v3.0, chiavi RSA a 1024 bit e crittografia RC4).
- Autorizzazione del traffico non criptato (HTTP) verso o da risorse pubbliche.
- Monitoraggio e sostituzione mancati dei certificati X.509 prima della scadenza.
- Utilizzo di certificati X.509 autofirmati per TLS.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

I servizi AWS forniscono endpoint HTTPS utilizzando TLS per le comunicazioni e offrono la crittografia in transito durante la comunicazione con le API AWS. I protocolli HTTP non sicuri possono essere sottoposti ad audit e bloccati in un cloud privato virtuale (VPC) tramite l'uso di gruppi di sicurezza. È possibile inoltre reindirizzare automaticamente in HTTPS le richieste HTTP in Amazon CloudFront o in un Application Load Balancer. Puoi utilizzare una policy dei bucket di Amazon Simple Storage Service (Amazon S3) per limitare la possibilità di caricare oggetti tramite HTTP, applicando efficacemente l'uso di HTTPS per il caricamento di oggetti nei tuoi bucket. Hai il controllo completo sulle tue risorse informatiche per implementare la crittografia in transito nei tuoi servizi. Inoltre, puoi

utilizzare la connettività VPN nel VPC da una rete esterna o AWS Direct Connect per semplificare la crittografia del traffico. Verifica che i tuoi client stiano effettuando chiamate alle API AWS utilizzando almeno TLS 1.2, poiché l'uso di versioni di TLS precedenti a febbraio 2024 è diventato obsoleto per AWS. Consigliamo di utilizzare TLS 1.3. Se hai requisiti speciali per la crittografia dei dati in transito, puoi trovare soluzioni di terze parti nel Marketplace AWS.

Passaggi dell'implementazione

- Applica la crittografia in transito: i requisiti di crittografia definiti dovrebbero essere basati sugli standard e sulle best practice più recenti e consentire solo protocolli sicuri. Ad esempio, configura un gruppo di sicurezza per consentire solo il protocollo HTTPS a un Application Load Balancer o a un'istanza Amazon EC2.
- Configura protocolli sicuri nei servizi edge: configura HTTPS con Amazon CloudFront e utilizza un profilo di sicurezza adeguato al tuo livello di sicurezza e il tuo caso d'uso.
- Usa una VPN per la connettività esterna: valuta l'impiego di una VPN IPsec per la protezione delle connessioni punto a punto o rete a rete al fine di garantire la riservatezza e l'integrità dei dati.
- Configura protocolli sicuri nei bilanciatori del carico: seleziona una policy di sicurezza che fornisca le suite di crittografia più solide supportate dai client che si connetteranno al listener. Create an HTTPS listener for your Application Load Balancer.
- Configura protocolli di sicurezza in Amazon Redshift: configura il cluster per richiedere una connessione Secure Socket Layer (SSL) o Transport Layer Security (TLS)..
- Configura protocolli sicuri: consulta la documentazione del servizio AWS per determinare le funzionalità di crittografia in transito.
- Configura l'accesso sicuro durante il caricamento su bucket Amazon S3: utilizza i controlli delle policy sui bucket Amazon S3 per applicare l'accesso sicuro ai dati.
- Prendi in considerazione l'utilizzo di AWS Certificate Manager: ACM ti consente di fornire, gestire e implementare certificati TLS pubblici da utilizzare con i servizi AWS.
- Prendi in considerazione l'utilizzo AWS Autorità di certificazione privata per le esigenze di PKI private: AWS Private CA consente di creare gerarchie di autorità di certificazione (CA) private per emettere certificati X.509 di entità finale, utilizzabili per creare canali TLS crittografati.

Risorse

Documenti correlati:

- Using HTTPS with CloudFront

- Connect your VPC to remote networks using AWS Virtual Private Network
- Create an HTTPS listener for your Application Load Balancer
- Tutorial: Configure SSL/TLS on Amazon Linux 2
- Using SSL/TLS to encrypt a connection to a DB instance
- Configuring security options for connections

SEC09-BP03 Autenticazione delle comunicazioni di rete

Verifica l'identità delle comunicazioni utilizzando protocolli che supportano l'autenticazione, ad esempio Transport Layer Security (TLS) o IPsec.

Progetta il carico di lavoro in modo da utilizzare protocolli di rete sicuri e autenticati per le comunicazioni tra servizi, applicazioni o utenti. L'utilizzo di protocolli di rete che supportano autenticazione e autorizzazione offre un controllo più rigido sui flussi di rete e riduce l'impatto di eventuali accessi non autorizzati.

Risultato desiderato: un carico di lavoro con un piano dati ben definito e flussi di traffico del piano di controllo (control-plane) tra i servizi. I flussi di traffico utilizzano protocolli di rete autenticati e crittografati laddove tecnicamente fattibile.

Anti-pattern comuni:

- Flussi di traffico non crittografati o non autenticati all'interno del carico di lavoro.
- Riutilizzo delle credenziali di autenticazione tra più utenti o entità.
- Uso esclusivo di controlli di rete come meccanismo di controllo degli accessi.
- Creazione di un meccanismo di autenticazione personalizzato anziché usare meccanismi di autenticazione standard del settore.
- Flussi di traffico eccessivamente permissivi tra i componenti del servizio o altre risorse nel VPC.

Vantaggi dell'adozione di questa best practice:

- Limita l'ambito dell'impatto di eventuali accessi non autorizzati a una parte del carico di lavoro.
- Fornisce un livello maggiore di sicurezza affinché solo entità autenticate eseguano le azioni.
- Migliora il disaccoppiamento dei servizi definendo e applicando in modo chiaro le interfacce di trasferimento dei dati previste.

- Migliora monitoraggio, creazione di log e risposta agli incidenti tramite l'attribuzione di richieste e interfacce di comunicazione ben definite.
- Fornisce una difesa approfondita ai carichi di lavoro combinando i controlli di rete con quelli di autenticazione e autorizzazione.

Livello di rischio associato se questa best practice non fosse adottata: basso

Guida all'implementazione

È possibile suddividere i modelli di traffico di rete del tuo carico di lavoro in due categorie:

- Il traffico est-ovest corrisponde ai flussi di traffico tra i servizi facenti parte di un carico di lavoro.
- Il traffico nord-sud rappresenta i flussi di traffico tra carico di lavoro e consumatori.

Sebbene crittografare il traffico nord-sud sia la prassi comune, proteggere il traffico est-ovest mediante protocolli autenticati non è così frequente. Le moderne best practice di sicurezza raccomandano che la progettazione della rete non sia l'unico elemento in grado di garantire una relazione affidabile tra due entità. Quando due servizi possono trovarsi all'interno di una rete comune, è comunque consigliabile crittografare, autenticare e autorizzare le comunicazioni tra tali servizi.

Ad esempio, le API del servizio AWS utilizzano il protocollo di firma AWSSignature Version 4 (SIGv4) per autenticare il chiamante, indipendentemente dalla rete di provenienza della richiesta. Questa autenticazione garantisce che le API di AWS possano verificare l'identità che ha richiesto l'azione e che tale identità possa quindi essere combinata con le policy per decidere se autorizzare o meno l'azione.

Servizi come Amazon VPC Lattice e Gateway Amazon API consentono di utilizzare lo stesso protocollo di firma SigV4 per aggiungere autenticazione e autorizzazione al traffico est-ovest nei propri carichi di lavoro. Se le risorse esterne al tuo ambiente AWS devono comunicare con servizi che richiedono autenticazione e autorizzazione basate su SigV4, puoi utilizzare AWS Identity and Access Management (IAM) Roles Anywhere sulla risorsa non AWS per acquisire credenziali AWS temporanee. Queste credenziali possono essere utilizzate per firmare richieste ai servizi che utilizzano SigV4 per autorizzare l'accesso.

Un altro meccanismo comune per l'autenticazione del traffico est-ovest è l'autenticazione reciproca TLS (mTLS). Molte applicazioni Internet delle cose (IoT), business-to-business (B2B) e microservizi utilizzano mTLS per convalidare l'identità di entrambi i lati di una comunicazione TLS mediante l'uso di certificati X.509 lato client e lato server. Questi certificati possono essere emessi da AWS Autorità

di certificazione privata (AWS Private CA). Puoi utilizzare servizi come Gateway Amazon API per garantire l'autenticazione mTLS per le comunicazioni interne ai carichi di lavoro o tra un carico di lavoro e un altro. Application Load Balancer supporta mTLS anche per i carichi di lavoro interni o esterni. Sebbene fornisca informazioni di autenticazione per entrambi i lati di una comunicazione TLS, mTLS non fornisce un meccanismo di autorizzazione.

Infine, OAuth 2.0 e OpenID Connect (OIDC) sono due protocolli in genere utilizzati per controllare l'accesso ai servizi da parte degli utenti, ma stanno diventando sempre più diffusi anche per il traffico da servizio a servizio. API Gateway fornisce un sistema di autorizzazione JSON Web token (JWT), che consente ai carichi di lavoro di limitare l'accesso ai percorsi API utilizzando JWT emessi da gestori dell'identità digitale OIDC o OAuth 2.0. È possibile utilizzare gli ambiti OAuth2 come base per decisioni di autorizzazione essenziali, ma i controlli di autorizzazione vanno comunque implementati a livello di applicazione. Gli ambiti OAuth2 da soli non possono supportare requisiti di autorizzazione più complessi.

Passaggi dell'implementazione

- Definisci e documenta i flussi di rete del carico di lavoro: il primo passo per implementare una strategia di difesa approfondita consiste nel definire i flussi di traffico del carico di lavoro.
  - Crea un diagramma del flusso di dati che definisca in modo chiaro le modalità di trasmissione dei dati tra i diversi servizi che costituiscono il carico di lavoro. Questo diagramma è il primo passo per autorizzare tali flussi nei canali di rete autenticati.
  - Nelle fasi di sviluppo e test dota il carico di lavoro di strumenti per controllare che il diagramma del flusso di dati rifletta in modo preciso il comportamento del carico di lavoro in fase di runtime.
  - Un diagramma di flusso di dati può essere utile anche quando si esegue un esercizio di modellazione delle minacce, come illustrato in SEC01-BP07 Identificare le minacce e dare priorità alle mitigazioni utilizzando un modello di minaccia.
- Stabilisci i controlli di rete: valuta le funzionalità di AWS per stabilire controlli di rete allineati ai flussi di dati. Sebbene non debbano costituire l'unico elemento di controllo della sicurezza, i confini della rete forniscono un livello nella strategia di difesa di alto profilo a protezione del carico di lavoro.
  - Utilizza i gruppi di sicurezza per stabilire, definire e limitare i flussi di dati tra le risorse.
  - Valuta l'utilizzo di AWS PrivateLink per comunicare sia con servizi AWS e di terze parti che supportano AWS PrivateLink. I dati inviati tramite un endpoint di interfaccia AWS PrivateLink rimangono all'interno della dorsale della rete AWS e non attraversano la rete Internet pubblica.
- Implementa autenticazione e autorizzazione tra i servizi del tuo carico di lavoro: scegli il set di servizi AWS più adeguato a fornire flussi di traffico autenticati e crittografati nel tuo carico di lavoro.

  - Prendi in considerazione Amazon VPC Lattice per proteggere la comunicazione da servizio a servizio. VPC Lattice può utilizzare l'autenticazione SigV4 in combinazione con le policy di autenticazione per controllare l'accesso da servizio a servizio.
  - Per la comunicazione da servizio a servizio tramite mTLS, prendi in considerazione API Gateway o Application Load Balancer. AWS Private CA consente di stabilire una gerarchia CA privata in grado di emettere certificati da utilizzare con mTLS.
  - In caso di integrazione con servizi che utilizzano OAuth 2.0 o OIDC, prendi in considerazione API Gateway mediante il sistema di autorizzazione JWT.
  - Per la comunicazione tra il carico di lavoro e i dispositivi IoT, prendi in considerazione AWS IoT Core, che offre diverse opzioni per la crittografia e l'autenticazione del traffico di rete.
- Monitora gli accessi non autorizzati: monitora in modo continuo i canali di comunicazione non intenzionali, i tentativi di accesso dei principali non autorizzati a risorse protette e altri schemi di accesso impropri.
  - Se utilizzi VPC Lattice per la gestione dell'accesso ai tuoi servizi, prendi in considerazione l'abilitazione e il monitoraggio dei log di accesso VPC Lattice. Questi log di accesso includono informazioni sull'entità richiedente, informazioni di rete tra cui VPC di origine e destinazione e metadati della richiesta.
  - Considera l'abilitazione dei log di flusso VPC per acquisire metadati sui flussi di rete e verificare a cadenza periodica la presenza di anomalie.
  - Consulta la AWS Security Incident Response Guide e la sezione Risposta agli imprevisti del pilastro della sicurezza del Framework AWS Well-Architected per ulteriori indicazioni su pianificazione, simulazione e risposta agli incidenti di sicurezza.

Risorse

Best practice correlate:

- SEC03-BP07 Analisi dell'accesso multi-account e pubblico
- SEC02-BP02 Utilizzo di credenziali temporanee
- SEC01-BP07 Identificare le minacce e dare priorità alle mitigazioni utilizzando un modello di minaccia

Documenti correlati:

- Evaluating access control methods to secure Amazon API Gateway APIs

- Configuring mutual TLS authentication for a REST API
- How to secure API Gateway HTTP endpoints with JWT authorizer
- Authorizing direct calls to AWS services using AWS IoT Core credential provider
- AWS Security Incident Response Guide

Video correlati:

- AWS re:invent 2022: Introducing VPC Lattice
- AWS re:invent 2020: Serverless API authentication for HTTP APIs on AWS

Esempi correlati:

- Amazon VPC Lattice Workshop
- Zero-Trust Episode 1 – The Phantom Service Perimeter workshop

Risposta agli incidenti

Anche se dispone di controlli preventivi e di rilevamento maturi, l'organizzazione deve ancora implementare meccanismi per rispondere e mitigare il potenziale impatto degli incidenti di sicurezza. La tua preparazione influisce fortemente sulla capacità dei team di operare in modo efficace durante un incidente, isolare, contenere ed eseguire indagini sui problemi e ripristinare le operazioni a uno stato valido noto. La messa in atto degli strumenti e l'accesso prima di un incidente di sicurezza, quindi la pratica sistematica della risposta agli incidenti durante le giornate di gioco, aiuterà a garantire il ripristino, riducendo al minimo le interruzioni dell'attività.

Argomenti

Aspetti della risposta agli incidenti di AWS

Tutti gli utenti AWS all'interno di un'organizzazione devono possedere una conoscenza di base dei processi di risposta agli incidenti di sicurezza e il personale addetto alla sicurezza deve capire come rispondere ai problemi di sicurezza. L'istruzione, la formazione e l'esperienza sono fondamentali per un programma di risposta agli incidenti nel cloud efficace e idealmente sono implementate con largo anticipo rispetto alla gestione di un possibile incidente di sicurezza. Le basi di un programma di risposta agli incidenti nel cloud efficace sono la preparazione, le operazioni e l'attività post-incidente.

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

- Preparazione: prepara il tuo team di risposta agli incidenti a rilevare e rispondere agli incidenti all'interno di AWS abilitando i controlli di rilevamento e verificando l'accesso appropriato per gli strumenti e ai servizi cloud necessari. Inoltre, prepara i playbook necessari, sia manuali sia automatizzati, per verificare che le risposte siano affidabili e coerenti.
- Operazioni: intraprendi azioni sugli eventi di sicurezza e sui potenziali incidenti seguendo le fasi di risposta agli incidenti del NIST (rilevamento, analisi, contenimento, rimozione e ripristino).

- Attività post-incidente: rifletti sull'esito degli eventi e delle simulazioni di sicurezza per migliorare l'efficacia della risposta, aumentare il valore derivante dalla risposta e dalle indagini e ridurre ulteriormente i rischi. Impara dagli incidenti e dimostra una forte responsabilità verso le attività di miglioramento.

Il diagramma seguente mostra il flusso di questi aspetti, in linea con il ciclo di vita della risposta agli incidenti del NIST menzionato in precedenza, ma include operazioni come il rilevamento e l'analisi oltre al contenimento, la rimozione e il ripristino.

Aspetti della risposta agli incidenti di AWS

Progettazione degli obiettivi di risposta al cloud

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

- Definizione degli obiettivi di risposta: collabora con le parti interessate, i consulenti legali e la leadership dell'organizzazione per determinare l'obiettivo di risposta a un incidente. Alcuni obiettivi comuni includono il contenimento e la mitigazione del problema, il recupero delle risorse interessate, la conservazione dei dati per le attività forensi, il ripristino delle operazioni sicure note e, in ultima analisi, l'apprendimento dagli incidenti.
- Risposte fornite utilizzando il cloud: implementa i tuoi modelli di risposta all'interno del cloud, dove si verificano l'evento e i dati.

- Scopri che cos'hai a disposizione e cosa ti serve: conserva log, risorse, snapshot e altre prove copiandole e archiviandole in un account cloud centralizzato dedicato alle risposte. Utilizza tag, metadati e meccanismi che applicano le policy di conservazione. Devi capire quali servizi utilizzi e quindi identificare i requisiti per esaminare tali servizi. Per aiutarti a comprendere il tuo ambiente, utilizza anche i tag.
- Utilizzo di meccanismi di reimplementazione: se un'anomalia di sicurezza può essere attribuita a una configurazione errata, la correzione potrebbe essere semplicemente rimuovere la varianza ridistribuendo le risorse con la configurazione corretta. Se viene identificato un possibile compromesso, verifica che la nuova implementazione includa una mitigazione efficace e verificata delle cause profonde.
- Automatizza laddove possibile: man mano che sorgono problemi o che gli incidenti si ripetono, crea meccanismi che verifichino e rispondano a eventi comuni a livello di programmazione. Usa le risposte umane per gestire incidenti unici, complessi o sensibili per i quali le automazioni sono insufficienti.
- Scegli soluzioni scalabili: cerca di associare la scalabilità dell'approccio della tua organizzazione al cloud computing. Implementa meccanismi di rilevamento e risposta dimensionabili nei tuoi ambienti per ridurre efficacemente il tempo che intercorre tra rilevamento e risposta.
- Impara e migliora i tuoi processi: identifica in maniera proattiva le lacune presenti nei tuoi processi, strumenti o persone e implementa un piano per colmarle. Le simulazioni sono metodi sicuri per individuare le lacune e migliorare i processi.

Questi obiettivi di progettazione sono un promemoria per rivedere l'implementazione dell'architettura al fine di migliorare la capacità di condurre sia la risposta agli incidenti sia il rilevamento delle minacce. Mentre pianifichi le tue implementazioni cloud, pensa a come rispondere a un incidente, idealmente utilizzando una metodologia di risposta valida dal punto di vista forense. In alcuni casi, ciò significa che potresti avere più organizzazioni, account e strumenti configurati specificamente per queste attività di risposta. Questi strumenti e funzioni devono essere messi a disposizione del team di risposta agli incidenti tramite una pipeline di implementazione. Non devono essere statici perché possono causare un rischio maggiore.

Preparazione

Essere preparati per affrontare un incidente è fondamentale per fornire una risposta tempestiva ed efficace. La preparazione viene effettuata in tre ambiti:

- Persone: la preparazione del personale per un incidente di sicurezza implica l'identificazione delle persone responsabili della risposta agli incidenti e la loro formazione in merito alle modalità di risposta e alle tecnologie cloud.
- Processi: la preparazione in termini di processi per un incidente di sicurezza implica la conoscenza della documentazione delle architetture, lo sviluppo di piani di risposta agli incidenti completi e la creazione di playbook per una risposta coerente agli eventi di sicurezza.
- Tecnologia: la preparazione in termini di tecnologia per un incidente di sicurezza implica la configurazione dell'accesso, l'aggregazione e il monitoraggio dei log necessari, l'implementazione di meccanismi di avviso efficaci e lo sviluppo di capacità di risposta e di indagine.

Ciascuno di questi domini è importante per una risposta efficace agli imprevisti. Nessun programma di risposta agli imprevisti è completo o efficace senza tutti e tre. Una preparazione agli incidenti può dirsi efficace solo se le persone, i processi e le tecnologie sono stati preparati in maniera adeguata e integrata.

Best practice

- SEC10-BP01 Identificazione del personale chiave e delle risorse esterne
- SEC10-BP02 Sviluppo di piani di gestione degli incidenti
- SEC10-BP03 Preparazione di funzionalità forensi
- SEC10-BP04 Sviluppo e test di playbook di risposta agli incidenti di sicurezza
- SEC10-BP05 Preassegnazione dell'accesso
- SEC10-BP06 Implementazione anticipata degli strumenti
- SEC10-BP07 Esecuzione di simulazioni

SEC10-BP01 Identificazione del personale chiave e delle risorse esterne

Identifica personale, risorse e requisiti legali interni ed esterni per consentire all'organizzazione a rispondere a un incidente.

Risultato desiderato: presenza di un elenco del personale chiave, delle relative informazioni di contatto e dei ruoli svolti nel rispondere a un evento di sicurezza. Rivedi queste informazioni con regolarità e aggiornarle per riflettere i cambiamenti del personale dal punto di vista degli strumenti interni ed esterni. Nel documentare queste informazioni, prendi in considerazione tutti i fornitori di servizi e i venditori di terze parti, compresi partner di sicurezza, fornitori di cloud e applicazioni

software-as-a-service (SaaS). Durante un evento di sicurezza, il personale è disponibile con il livello di responsabilità, il contesto e l'accesso appropriati per poter rispondere ed eseguire il ripristino.

Anti-pattern comuni:

- Mancata tenuta di un elenco aggiornato del personale chiave con le informazioni di contatto, i ruoli e le responsabilità in caso di risposta a eventi di sicurezza.
- Si presume che tutti conoscano persone, dipendenze, infrastruttura e soluzioni per rispondere a un evento ed eseguire il ripristino dopo lo stesso.
- Mancata predisposizione di un archivio di documenti o conoscenze che rappresenti l'infrastruttura o la progettazione di applicazioni chiave.
- Mancata predisposizione di processi di onboarding adeguati per i nuovi dipendenti, in modo che possano contribuire in modo efficace alla risposta a un evento di sicurezza, come la realizzazione di simulazioni di eventi.
- Mancata predisposizione di un percorso di escalation quando il personale chiave è temporaneamente non disponibile o non risponde durante gli eventi di sicurezza.

Vantaggi dell'adozione di questa best practice: riduzione del tempo di valutazione e risposta impiegato per identificare il personale giusto e il relativo ruolo durante un evento grazie a questa pratica. Riduci al minimo le perdite di tempo durante un evento mantenendo un elenco aggiornato del personale chiave e dei relativi ruoli, in modo da poter portare le persone giuste al triage e al ripristino da un evento.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all’implementazione

Identifica il personale chiave all'interno dell'organizzazione: conserva un elenco di contatti del personale interno alla tua organizzazione che potrebbe essere necessario coinvolgere. Rivedi e aggiorna in modo regolare queste informazioni in caso di spostamento del personale, quali modifiche organizzative, promozioni e cambi di team. Questo è particolarmente importante per i ruoli chiave come gli incident manager, i team di risposta e i responsabili delle comunicazioni.

- Responsabile degli incidenti: i responsabili degli incidenti dispongono dell'autorità generale durante la risposta all'evento.
- Persone che intervengono dopo un incidente: le persone che intervengono dopo un incidente sono responsabili delle attività di indagine e correzione. Queste persone possono differire in base

al tipo di evento, ma in genere sono sviluppatori e team operativi responsabili dell'applicazione interessata.

- Responsabile delle comunicazioni: il responsabile delle comunicazioni gestisce comunicazioni interne ed esterne, in particolare con gli enti pubblici, le autorità di regolamentazione e i clienti.
- Processo di onboarding: attività periodiche di formazione e onboarding per i nuovi dipendenti, mirate a fornire le competenze e le conoscenze necessarie per dare un contributo efficace alle iniziative di risposta agli incidenti. Include simulazioni ed esercizi pratici nell'ambito del processo di onboarding per facilitarne la preparazione.
- Esperti in materia (SME): in caso di team distribuiti e autonomi, ti consigliamo di identificare un SME per carichi di lavoro mission critical. Queste persone offrono approfondimenti su funzionamento e classificazione dei dati dei carichi di lavoro critici coinvolti nell'evento.

Formato di tabella di esempio:

```
  | Role | Name | Contact Information | Responsibilities |
1 | ——- | ——- | ——- | ——- |
2 | Incident Manager | Jane Doe| jane.doe@example.com | Overall authority during
 response |
3 | Incident Responder | John Smith | john.smith@example.com | Investigation and
 remediation |
4 | Communications Lead | Emily Johnson | emily.johnson@example.com | Internal and
 external communications |
5 | Communications Lead | Michael Brown | michael.brown@example.com | Insights on
 critical workloads |
```

Prendi in considerazione l'utilizzo della funzionalità AWS Systems Manager Incident Manager per l'acquisizione dei contatti chiave, la definizione di un piano di risposta, l'automazione degli orari delle chiamate e la creazione di piani di escalation. Automatizza e organizza i turni per tutto il personale attraverso un programma di chiamata, in modo che la responsabilità del carico di lavoro sia condivisa tra i proprietari. Ciò promuove buone pratiche, come l'emissione di metriche e log pertinenti e la definizione di soglie di allarme importanti per il carico di lavoro.

Identifica i partner esterni: le aziende utilizzano strumenti creati da fornitori di software indipendenti (ISV), partner e subappaltatori per creare soluzioni differenziate per i propri clienti. Coinvolgi il personale chiave di queste parti che può aiutarti a rispondere e a eseguire il ripristino dopo un incidente. Ti consigliamo di iscriverti al livello appropriato di Supporto per ottenere un rapido accesso agli SME AWS attraverso un caso di supporto. Prendi in considerazione accordi simili con tutti i fornitori di soluzioni critiche per i carichi di lavoro. Alcuni eventi di sicurezza richiedono alle aziende

quotate in borsa di notificare evento ed effetti agli enti pubblici e alle autorità di regolamentazione pertinenti. Mantieni e aggiorna le informazioni di contatto per i dipartimenti pertinenti e le persone responsabili.

Passaggi dell'implementazione

1. Configura una soluzione per la gestione degli incidenti.
   a. Prendi in considerazione l'implementazione di Incident Manager nel tuo account Security Tooling.
2. Definisci i contatti nella tua soluzione di gestione degli incidenti.
   a. Definisci almeno due tipi di canali per ogni contatto (come SMS, telefono o e-mail), per garantire la raggiungibilità durante un incidente.
3. Definisci un piano di risposta.
   a. Identifica i contatti più opportuni da coinvolgere durante un incidente. Definisci piani di escalation in linea con i ruoli del personale da coinvolgere, piuttosto che con i singoli contatti. Valuta la possibilità di includere i contatti che potrebbero essere responsabili dell'informare entità esterne, anche se non direttamente coinvolti nella risoluzione dell'incidente.

Risorse

Best practice correlate:

- OPS02-BP03 Assegnazione di proprietari identificati alle operazioni che siano responsabili delle relative prestazioni

Documenti correlati:

- AWS Security Incident Response Guide

Esempi correlati:

- AWS Framework per playbook per i clienti
- Prepare for and respond to security incidents in your AWS environment

Strumenti correlati:

- AWS Systems Manager Incident Manager

Video correlati:

- Amazon's approach to security during development

SEC10-BP02 Sviluppo di piani di gestione degli incidenti

Il primo documento da predisporre per la risposta agli incidenti è il piano di risposta agli incidenti. Lo scopo del piano di risposta agli incidenti è costituire la base del programma e della strategia di risposta agli incidenti.

Vantaggi dell'adozione di questa best practice: lo sviluppo di processi di risposta agli incidenti completi e definiti in modo chiaro è fondamentale per un programma di risposta agli incidenti efficace e scalabile. Quando si verifica un evento di sicurezza, passaggi e flussi di lavoro ben definiti agevoleranno una risposta tempestiva. Potrebbero essere già presenti processi di risposta agli incidenti. Indipendentemente dallo stato attuale, è importante aggiornare, iterare e testare con regolarità i processi di risposta agli incidenti.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Un piano di gestione degli incidenti è fondamentale per rispondere, mitigare ed eseguire il ripristino a seguito del potenziale impatto degli incidenti di sicurezza. Un piano di gestione degli incidenti è un processo strutturato volto a identificare, correggere e rispondere tempestivamente agli incidenti di sicurezza.

Il cloud presenta molti degli stessi ruoli e requisiti operativi che si trovano in un ambiente on-premises. Nella creazione di un piano di gestione degli incidenti, è importante tenere conto delle strategie di risposta e ripristino ideali per i risultati aziendali e ai requisiti di conformità. Ad esempio, se gestisci carichi di lavoro in AWS conformi a FedRAMP negli Stati Uniti, occorre seguire le raccomandazioni enunciate nel documento NIST SP 800-61 Computer Security Handling Guide. Allo stesso modo, quando gestisci carichi di lavoro che memorizzano informazioni di identificazione personale (PII), valuta come proteggere e rispondere ai problemi relativi alla residenza e all'utilizzo dei dati.

Quando crei un piano di gestione degli incidenti per i tuoi carichi di lavoro in AWS, inizia con il modello di responsabilità condivisa AWS per creare un approccio di difesa approfondito alla risposta

agli incidenti. In questo modello, AWS gestisce la sicurezza del cloud e tu sei responsabile della sicurezza nel cloud. Ciò significa che mantieni il controllo e sei responsabile dei controlli di sicurezza che scegli di implementare. La AWS Security Incident Response Guide illustra concetti chiave e linee guida di base per la creazione di un piano di gestione degli incidenti incentrato sul cloud.

Un piano di gestione degli incidenti efficace va iterato in modo continuo per rimanere in linea con l'obiettivo delle operazioni cloud. Prendi in considerazione l'utilizzo dei piani di implementazione illustrati di seguito durante la creazione e l'evoluzione del tuo piano di gestione degli incidenti.

Passaggi dell'implementazione

1. Definisci ruoli e responsabilità all'interno dell'organizzazione per la gestione degli eventi di sicurezza. Il processo dovrebbe coinvolgere rappresentanti di vari dipartimenti, tra cui:
   - Risorse umane (HR)
   - Team esecutivo
   - Ufficio legale
   - Proprietari e sviluppatori di applicazioni (SME, ossia esperti in materia)
2. Determina in modo chiaro i soggetti RACI (Responsible, Accountable, Consulted, and Informed) da tenere in considerazione in caso di incidente. Crea un grafico RACI per facilitare una comunicazione rapida e diretta, e delinea chiaramente la leadership nelle diverse fasi di un evento.
3. Coinvolgi i proprietari e gli sviluppatori delle applicazioni (SME) durante un incidente, poiché tali soggetti possono fornire informazioni e contesto preziosi per aiutare a misurare l'impatto. Instaura relazioni con questi SME e fai pratica con loro utilizzando vari scenari di risposta agli incidenti prima che si verifichi un incidente reale.
4. Coinvolgi partner attendibili o esperti esterni nel processo di indagine o risposta, poiché tali soggetti possono fornire competenze e prospettive aggiuntive.
5. Allinea i piani e i ruoli di gestione degli incidenti alle normative locali o ai requisiti di conformità che regolano la tua organizzazione.
6. Effettua regolarmente esercitazioni pratiche e test sui piani di risposta agli incidenti, coinvolgendo tutti i ruoli e le responsabilità definiti. Questo aiuta a semplificare il processo e ad assicurarsi di avere una risposta coordinata ed efficiente agli incidenti di sicurezza.
7. Rivedi e aggiorna i ruoli, le responsabilità e il grafico RACI periodicamente o man mano che la struttura organizzativa o i requisiti cambiano.

Analizza il supporto e i team di risposta di AWS

- Supporto AWS
  - Supporto offre un'ampia gamma di piani che forniscono accesso agli strumenti e alla competenza che genera successo e stato operativo delle soluzioni AWS. Se ti occorre supporto tecnico e ulteriori risorse per pianificare, implementare e ottimizzare il tuo ambiente AWS, puoi selezionare il piano di supporto più adatto al tuo caso d'uso AWS.
  - Considera il Centro supporto in Console di gestione AWS (è richiesto l'accesso) come punto di contatto centralizzato per assistenza circa problemi relativi alle tue risorse AWS. L'accesso a Supporto è controllato da AWS Identity and Access Management. Per ulteriori informazioni sull'accesso alle funzionalità Supporto, consulta Getting started with Supporto.
- AWS Team di risposta agli incidenti dei clienti (CIRT)
  - Il Team di risposta agli incidenti dei clienti AWS (CIRT) è un team AWS globale specializzato, disponibile 24 ore su 24, 7 giorni su 7, che fornisce supporto ai clienti durante eventi di sicurezza attivi sul lato cliente del modello di responsabilità condivisa di AWS.
  - Quando il team AWS CIRT ti supporta, fornisce assistenza nella valutazione e nel ripristino di un evento di sicurezza su AWS. Può fornire assistenza nell'analisi delle cause principali grazie all'uso dei log dei servizi AWS e fornire suggerimenti per il ripristino. Può altresì fornire consigli e best practice sulla sicurezza così da evitare eventi di sicurezza in futuro.
  - I clienti AWS possono rivolgersi al team AWS CIRT attraverso un caso Supporto.
- AWS Security Incident Response
  - Annunciato al re:Invent 2024, AWS Security Incident Response è un servizio gestito di risposta agli incidenti di sicurezza che utilizza sia la moderna tecnologia di triage che un operatore umano presente nel loop. Il servizio acquisisce tutti gli esiti di GuardDuty e tutti gli esiti di terze parti inviati a AWS Security Hub CSPM per la valutazione al fine di avvisare il cliente solo degli esiti che richiedono un'indagine. Il servizio fornisce anche un portale per presentare casi reattivi in caso di un evento di sicurezza notato dal cliente e ricevere supporto dal team di risposta avanzata agli incidenti di AWS.
- Supporto per la risposta agli attacchi DDoS
  - AWS offre AWS Shield, un servizio gestito di protezione da attacchi di tipo DDoS (Distributed Denial of Service) che protegge le applicazioni Web in esecuzione in AWS. Shield fornisce un rilevamento continuo e prevenzione incorporata automatica che riducono al minimo il tempo di inattività e la latenza dell'applicazione, così da non dover rivolgersi al Supporto per beneficiare della protezione DDoS. I livelli esistenti di Shield sono due: AWS Shield Standard e AWS Shield Advanced. Per maggiori informazioni sulle differenze tra questi due livelli, consulta la documentazione della funzionalità Shield.

- AWS Managed Services (AMS)
  - AWS Managed Services (AMS) offre una gestione continua dell'infrastruttura AWS, così potrai concentrarti solo sulle tue applicazioni. Grazie all'implementazione di best practice per la manutenzione dell'infrastruttura, AMS consente di ridurre rischi e costi operativi. AMS automatizza attività frequenti quali richieste di modifica, monitoraggio, gestione di patch, sicurezza e backup, nonché fornisce servizi completi per il ciclo di vita per gestire provisioning, esecuzione e supporto dell'infrastruttura.
  - AMS è responsabile dell'implementazione di una suite di controlli di sicurezza e fornisce una risposta di prima linea agli avvisi 24 ore su 24, 7 giorni su 7. In caso di avviso, AMS si attiene a una serie standard di playbook automatici e manuali per verificare una risposta coerente. Questi playbook vengono condivisi con i clienti AMS durante l'onboarding in modo che possano sviluppare e coordinare una risposta con AMS.

Sviluppo di piani di risposta agli incidenti

Lo scopo del piano di risposta agli incidenti è costituire la base del programma e della strategia di risposta agli incidenti. Il piano di risposta agli incidenti deve essere contenuto in un documento formale. Un piano di risposta agli incidenti include in genere le seguenti sezioni:

- Una panoramica del team di risposta agli incidenti: delinea obiettivi e funzioni del team di risposta agli incidenti.
- Ruoli e responsabilità: indica le parti interessate alla risposta agli incidenti e illustra in dettaglio i loro ruoli in caso di incidente.
- Un piano di comunicazione: fornisce dettagli sulle informazioni di contatto e sulle tue modalità di comunicazione durante un incidente.
- Metodi di comunicazione di backup: è consigliabile utilizzare la comunicazione fuori banda come backup in caso di incidente. Un esempio di applicazione che fornisce un canale di comunicazione fuori banda sicuro è AWS Wickr.
- Fasi di risposta agli incidenti e azioni da intraprendere: elenca le fasi della risposta agli incidenti (ad esempio, rilevamento, analisi, eliminazione, contenimento e ripristino), comprese le azioni di alto livello da intraprendere all'interno di tali fasi.
- Definizioni di gravità e assegnazione della priorità agli incidenti: illustra in dettaglio come classificare la gravità di un incidente, le modalità di assegnazione della priorità all'incidente e, quindi, in che modo le definizioni di gravità influiscono sulle procedure di escalation.

Sebbene queste sezioni siano comuni ad aziende di diverse dimensioni e settori, il piano di risposta agli incidenti di ciascuna organizzazione è unico. Devi creare un piano di risposta agli incidenti che funzioni al meglio per la tua organizzazione.

Risorse

Best practice correlate:

- SEC04 Rilevamento

Documenti correlati:

- AWS Security Incident Response Guide
- NIST: Computer Security Incident Handling Guide

SEC10-BP03 Preparazione di funzionalità forensi

Prima che si verifichi un incidente di sicurezza, puoi sviluppare funzionalità forensi per supportare le indagini sugli eventi di sicurezza.

Livello di rischio associato se questa best practice non fosse adottata: medio

Il concetto della tradizionale analisi forense on-premises si applica ad AWS. Per informazioni chiave su come iniziare a sviluppare funzionalità forensi in Cloud AWS, consulta Forensic investigation environment strategies in the Cloud AWS.

Una volta configurati ambiente e struttura di Account AWS per le funzionalità forensi, definisci le tecnologie necessarie in modo da eseguire in modo ottimale le metodologie forensi in quattro fasi:

- Raccolta: raccogli i log AWS pertinenti, come quelli di AWS CloudTrail, AWS Config, del flusso VPC e dell'host. Raccogli snapshot, backup e dump di memoria delle risorse AWS interessate, se disponibili.
- Esame: rivedi i dati raccolti estraendo e valutando le informazioni pertinenti.
- Analisi: analizza i dati raccolti per comprendere l'incidente e trarre le conclusioni.
- Creazione di report: presenta le informazioni risultanti dalla fase di analisi.

Passaggi dell'implementazione

Preparazione dell'ambiente per le funzionalità forensi

AWS Organizations ti aiuta a gestire e dirigere a livello centrale un ambiente AWS mentre le risorse AWS crescono e scalano. Un'organizzazione AWS consolida gli Account AWS in modo da poterli amministrare come una singola unità. Puoi utilizzare le unità organizzative (UO) per raggruppare gli account e amministrarli come singola unità.

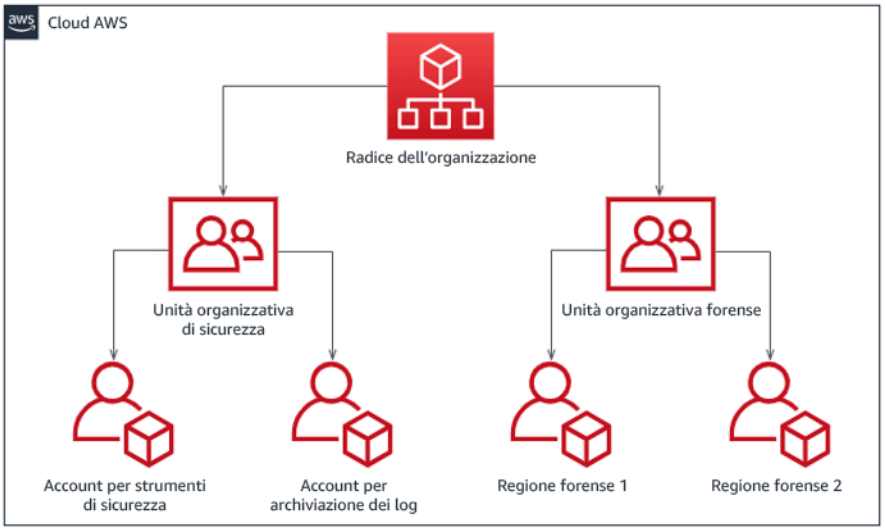
Per rispondere agli incidenti, è utile disporre di una struttura di Account AWS che supporti le funzioni di risposta agli incidenti e includa un'unità organizzativa di sicurezza e un'unità organizzativa con funzionalità forensi. All'interno dell'unità organizzativa di sicurezza, è necessario disporre degli account per:

- Archiviazione dei log: aggrega i log in un Account AWS di archiviazione dei log con autorizzazioni limitate.
- Strumenti di sicurezza: centralizza i servizi di sicurezza in un Account AWS dello strumento di sicurezza. Questo account funge da amministratore delegato per i servizi di sicurezza.

Nell'unità organizzativa con funzionalità forensi, puoi implementare uno o più account con funzionalità forensi per ciascuna regione in cui operi, a seconda di quale è più adatta all'azienda e al modello operativo. Se crei un account con funzionalità forensi per regione, puoi bloccare la creazione di risorse AWS al di fuori della regione e ridurre il rischio di copia delle risorse in una regione indesiderata. Ad esempio, se operi solo nella regione degli Stati Uniti orientali (Virginia settentrionale) (`us-east-1`) e Stati Uniti occidentali (Oregon) (`us-west-2`), nell'unità organizzativa con funzionalità forensi avrai due account: uno per `us-east-1` e uno per `us-west-2`.

Puoi creare un Account AWS con funzionalità forensi per più regioni. Quando si copiano le risorse AWS nell'account, presta attenzione a rispettare i requisiti di sovranità dei dati. Poiché la creazione di nuovi account richiede tempo, è fondamentale creare e fornire gli strumenti adatti agli account con funzionalità forensi con largo anticipo rispetto agli incidenti, in modo che gli addetti siano preparati a utilizzarli in modo efficace per la risposta.

Il diagramma seguente mostra una struttura degli account di esempio che include un'unità organizzativa con funzionalità forensi con account con funzionalità forensi per regione:



Struttura degli account per regione per la risposta agli incidenti

Acquisizione di backup e snapshot

La configurazione dei backup di sistemi e database importanti è fondamentale per il ripristino da un incidente di sicurezza e per scopi forensi. Grazie ai backup puoi ripristinare i tuoi sistemi allo stato di sicurezza precedente. In AWS puoi acquisire snapshot di varie risorse. Gli snapshot forniscono i backup point-in-time delle risorse. Esistono molti servizi AWS che offrono supporto nelle operazioni di backup e ripristino. Per informazioni dettagliate su questi servizi e approcci per il backup e il ripristino, consulta la guida prescrittiva per il backup e il ripristino e Use backups to recover from security incidents.

Soprattutto in situazioni come un attacco ransomware, è fondamentale che i backup siano ben protetti. Per indicazioni sulla protezione dei backup, consulta Top 10 security best practices for securing backups in AWS. Oltre a proteggere i backup, è necessario sottoporli regolarmente a processi di backup e ripristino per verificare che tecnologia e procedure in uso funzionino come previsto.

Automazione delle funzionalità forensi

Durante un evento di sicurezza, il team addetto a rispondere agli incidenti deve essere in grado di raccogliere e analizzare rapidamente le prove, mantenendo la precisione per il periodo di tempo relativo all'evento (ad esempio, acquisendo i log relativi a una risorsa o un evento specifico o raccogliendo il dump della memoria di un'istanza Amazon EC2). Per il team addetto a rispondere agli incidenti è difficile e dispendioso in termini di tempo raccogliere manualmente le prove pertinenti, soprattutto se istanze e account sono numerosi. Inoltre, la raccolta manuale può essere soggetta

all'errore umano. Per questi motivi, occorre sviluppare e implementare il più possibile l'automazione per le funzionalità forensi.

AWS offre una serie di risorse di automazione per le funzionalità forensi, elencate nella sezione Risorse più avanti. Queste risorse sono esempi di modelli di funzionalità forensi che abbiamo sviluppato, implementate dai clienti Sebbene costituiscano un'utile architettura di riferimento per iniziare, prendi in considerazione la possibilità di modificarli o creare nuovi modelli di automazione per le funzionalità forensi in base ad ambiente, requisiti, strumenti e processi forensi.

Risorse

Documenti correlati:

- AWS Security Incident Response Guide - Develop Forensics Capabilities
- AWS Security Incident Response Guide - Forensics Resources
- Forensic investigation environment strategies in the Cloud AWS
- How to automate forensic disk collection in AWS
- AWS Prescriptive Guidance - Automate incident response and forensics

Video correlati:

- Automating Incident Response and Forensics

Esempi correlati:

- Automated Incident Response and Forensics Framework
- Automated Forensics Orchestrator for Amazon EC2

SEC10-BP04 Sviluppo e test di playbook di risposta agli incidenti di sicurezza

Una parte fondamentale della preparazione dei processi di risposta agli incidenti è costituita dalla predisposizione di playbook. I playbook di risposta agli incidenti forniscono indicazioni prescrittive e passaggi da seguire in caso di evento di sicurezza. Una struttura e passaggi chiari semplificano la risposta e riducono la probabilità di errore umano.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

È necessario creare i playbook per scenari di incidenti come:

- Incidenti previsti: i playbook devono essere creati per gli incidenti previsti, tra cui minacce come Denial of Service (DoS), ransomware e la compromissione delle credenziali.
- Avvisi o esiti di sicurezza noti: i playbook devono essere creati per affrontare gli esiti e gli avvisi di sicurezza noti, ad esempio quelli di Amazon GuardDuty. Quando ricevi un esito di GuardDuty, il playbook dovrebbe fornire istruzioni chiare per evitare che l'avviso venga gestito in modo errato o ignorato. Per ulteriori dettagli e indicazioni sulla riparazione, consulta Correzione dei problemi di sicurezza rilevati da GuardDuty.

I playbook devono contenere i passaggi tecnici che un analista della sicurezza deve seguire per indagare e rispondere in modo adeguato a un potenziale incidente di sicurezza.

Il Customer Incident Response Team (CIRT) di AWS ha pubblicato un repository GitHub contenente i playbook di risposta agli incidenti, organizzati per scenario, tipo e risorsa delle minacce. Questi playbook possono essere adattati per allinearsi alle procedure di risposta agli incidenti esistenti o fungere da base per svilupparne di nuove.

Passaggi dell'implementazione

Gli elementi da includere in un playbook sono:

- Panoramica del playbook: quale scenario di rischio o incidente affronta questo playbook? Qual è l'obiettivo del playbook?
- Prerequisiti: quali log, meccanismi di rilevamento e strumenti automatizzati sono necessari per questo scenario di incidente? Qual è la notifica prevista?
- Informazioni su comunicazione ed escalation: chi è coinvolto e quali sono le sue informazioni di contatto? Quali sono le responsabilità di ciascuna parte interessata?
- Passaggi di risposta: in tutti i passaggi per la risposta agli incidenti, quali misure tattiche devono essere prese? Quali query deve eseguire l'analista? Quale codice va eseguito per ottenere il risultato desiderato?
  - Individuazione: come verrà individuato l'incidente?
  - Analisi: come verrà determinato l'ambito dell'impatto?
  - Contenimento: come verrà isolato l'incidente per limitarne la portata?
  - Sradicamento: come verrà rimossa la minaccia dall'ambiente?

  - Ripristino: in che modo il sistema o la risorsa interessati verranno riportati in produzione?
- Risultati previsto: dopo l'esecuzione delle query e del codice, qual è il risultato previsto del playbook?

Risorse

Best practice Well-Architected correlate:

- SEC10-BP02 Sviluppo di piani di gestione degli incidenti

Documenti correlati:

- Framework for Incident Response Playbooks
- Develop your own Incident Response Playbooks
- Incident Response Playbook Samples
- Building an AWS incident response runbook using Jupyter playbooks and CloudTrail Lake

SEC10-BP05 Preassegnazione dell'accesso

Verifica che le persone che intervengono dopo un incidente dispongano degli opportuni diritti di accesso allocati in AWS, così da ridurre i tempi necessari per l'analisi e il ripristino.

Anti-pattern comuni:

- Utilizzo dell'account root per la risposta agli incidenti.
- Modifica degli account utente esistenti.
- Manipolazione diretta delle autorizzazioni IAM quando si fornisce l'elevazione dei privilegi just-in-time.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

AWS raccomanda di ridurre o eliminare, ove possibile, la dipendenza da credenziali di lunga durata, a favore delle credenziali temporanee e dei meccanismi di escalation dei privilegi just-in-time. Le

credenziali di lunga durata sono soggette a rischi per la sicurezza e aumentano il sovraccarico operativo. Per la maggior parte delle attività di gestione, nonché per quelle di risposta agli incidenti, si consiglia di implementare la federazione delle identità insieme all'escalation temporanea per l'accesso amministrativo. In questo modello, un utente richiede l'elevazione a un livello di privilegio superiore (come un ruolo di risposta agli incidenti) e, se è idoneo all'elevazione, la richiesta viene inviata al responsabile dell'approvazione. In caso di approvazione della richiesta, l'utente riceve una serie di credenziali AWS temporanee, utilizzabili per completare le proprie attività. Alla scadenza di tali credenziali, l'utente deve inviare una nuova richiesta di elevazione.

Si consiglia l'uso dell'escalation temporanea dei privilegi nella maggior parte degli scenari di risposta agli incidenti. Il modo corretto per eseguire questa operazione prevede l'utilizzo di AWS Security Token Service e policy di sessione per definire l'ambito dell'accesso.

Esistono scenari in cui le identità federate non sono disponibili, come nei seguenti casi:

- Interruzione correlata a un gestore dell'identità digitale (IdP) compromesso.
- Configurazione errata o errore umano che causa l'interruzione del sistema di gestione dell'accesso federato.
- Attività dannose, come un evento DDoS (Distributed Denial of Service) o l'indisponibilità del sistema.

Nei casi precedenti, occorre configurare l'accesso di emergenza break glass in modo da consentire l'indagine e la risoluzione tempestiva degli incidenti. È consigliabile ricorrere a utenti, gruppi o ruoli con le autorizzazioni opportune per l'esecuzione delle attività e l'accesso alle risorse AWS. Ricorri all'utente root solo per le attività che richiedono le credenziali dell'utente root. Per verificare che le persone che intervengono dopo un incidente dispongano del corretto livello di accesso ad AWS e ad altri sistemi pertinenti, ti consigliamo di eseguire la preallocazione di account dedicati. Gli account richiedono l'accesso con privilegi e devono essere rigorosamente controllati e monitorati. Gli account vanno creati con il minor numero di privilegi richiesti per eseguire le attività e il livello di accesso deve essere basato sui playbook inclusi nel piano di gestione degli incidenti.

Ricorri a utenti e ruoli specifici e dedicati come best practice. L'escalation temporanea dell'accesso di utenti o ruoli tramite l'aggiunta di policy IAM rende poco chiaro quale fosse l'accesso degli utenti durante l'incidente e si rischia la mancata revoca dei privilegi oggetto di escalation.

È importante rimuovere il maggior numero possibile di dipendenze per verificare che sia possibile ottenere l'accesso nel maggior numero possibile di scenari di errore. A supporto di ciò, crea un playbook per verificare che gli utenti di risposta agli incidenti vengano creati come utenti in un

account di sicurezza dedicato e non gestiti tramite una federazione esistente o una soluzione di autenticazione Single Sign-On (SSO) Ogni singola persona che interviene dopo un incidente deve avere il proprio account denominato. La configurazione dell'account deve applicare una policy delle password complesse e l'autenticazione a più fattori (MFA). Se i playbook di risposta agli incidenti richiedono solo l'accesso al Console di gestione AWS, non è necessario che l'utente disponga di chiavi di accesso configurate né che sia esplicitamente autorizzato a creare chiavi di accesso. Questo può essere configurato con policy IAM o policy di controllo dei servizi come menzionato nelle best practice di sicurezza di AWS per le AWS Organizations SCP. Gli utenti non devono disporre di privilegi oltre alla capacità di assumere i ruoli di risposta agli incidenti in altri account.

Durante un incidente, potrebbe essere necessario concedere l'accesso ad altre persone interne o esterne per supportare le attività di analisi, correzione o ripristino. In questo caso, utilizza il meccanismo del playbook menzionato in precedenza e un processo per verificare la revoca immediata di qualsiasi accesso aggiuntivo immediatamente dopo la risoluzione dell'incidente.

Per verificare che l'uso dei ruoli di risposta agli incidenti possa essere adeguatamente monitorato e sottoposto ad audit, è essenziale che gli account IAM creati a tale scopo non siano condivisi tra le persone e che non si faccia ricorso all'Utente root dell'account AWS, salvo che non sia necessario per un'attività specifica. Se è richiesto l'utente root (ad esempio, l'accesso IAM a un account specifico non è disponibile), utilizza un processo separato con un playbook disponibile per verificare la disponibilità delle credenziali di accesso dell'utente root e del token MFA.

Per configurare le policy IAM per i ruoli di risposta agli incidenti, prendi in considerazione l'utilizzo di IAM Access Analyzer per generare policy basate su log AWS CloudTrail. In questo caso, concedi l'accesso come amministratore al ruolo di risposta agli incidenti per un account non di produzione e segui i playbook. Al termine, potrà essere creata una policy che consenta solo le azioni da intraprendere. Questa policy potrà quindi essere applicata a tutti i ruoli di risposta agli incidenti in tutti gli account. Puoi anche creare una policy IAM separata per ciascun playbook per semplificare gestione e audit. Esempi di playbook possono essere piani di risposta per ransomware, violazioni dei dati, perdita dell'accesso alla produzione e altri scenari.

Utilizza gli account di risposta agli incidenti per assumere i ruoli IAM dedicati di risposta agli incidenti in altri Account AWS. Questi ruoli devono essere configurati in modo che possano essere assunti solo dagli utenti nell'account di sicurezza e la relazione di trust deve richiedere che il principale chiamante sia autenticato tramite MFA. I ruoli devono utilizzare policy IAM con ambito limitato per controllare l'accesso. Assicurati che tutte le richieste `AssumeRole` per questi ruoli vengano registrate in CloudTrail e notificate e che tutte le azioni intraprese utilizzando questi ruoli vengano registrate.

Ti consigliamo vivamente di denominare in modo chiaro gli account IAM e i ruoli IAM per trovarli facilmente nei log di CloudTrail. Un esempio potrebbe essere quello di denominare gli account IAM *<USER_ID>*-BREAK-GLASS e i ruoli IAM BREAK-GLASS-ROLE.

CloudTrail consente di creare log dell'attività delle API negli account AWS e va utilizzato per configurare gli avvisi sull'utilizzo dei ruoli di risposta agli incidenti. Fai riferimento al post del blog sulla configurazione degli avvisi quando vengono utilizzate le chiavi root. È possibile modificare le istruzioni in modo da configurare la metrica da filtro a filtro di Amazon CloudWatch sugli eventi AssumeRole relativi al ruolo IAM di risposta agli incidenti:

```
{ $.eventName = "AssumeRole" && $.requestParameters.roleArn =
 "<INCIDENT_RESPONSE_ROLE_ARN>" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !
= "AwsServiceEvent" }
```

Vista la probabilità che i ruoli di risposta agli incidenti abbiano un livello di accesso elevato, è importante che questi avvisi vengano inviati a un gruppo ampio e gestiti tempestivamente.

Durante un incidente, è possibile che un membro del team di risposta richieda l'accesso a sistemi non direttamente protetti da IAM, ad esempio istanze Amazon Elastic Compute Cloud, database del servizio Amazon Relational Database o piattaforme Software-as-a-Service (SaaS). Si consiglia di utilizzare AWS Systems Manager Session Manager, anziché protocolli nativi come SSH o RDP per tutti gli accessi amministrativi alle istanze di Amazon EC2. Questo accesso può essere monitorato utilizzando IAM, che è sicuro e controllato. È inoltre possibile automatizzare parti dei playbook mediante i documenti AWS Systems Manager Run Command, in modo da ridurre gli errori degli utenti e migliorare i tempi di ripristino. Per l'accesso a database e strumenti di terze parti, ti consigliamo di archiviare le credenziali di accesso in Gestione dei segreti AWS e di concedere l'accesso ai ruoli delle persone che intervengono dopo gli incidenti.

Infine, la gestione degli account IAM per la risposta agli incidenti dovrebbe essere aggiunta ai processi degli utenti che si uniscono, si spostano o lasciano l'organizzazione e va riesaminata e testata periodicamente per verificare che sia consentito solo l'accesso previsto.

Risorse

Documenti correlati:

- Managing temporary elevated access to your AWS environment
- AWS Security Incident Response Guide
- Ripristino di emergenza di elastico di AWS

- Strumento di gestione degli incidenti AWS Systems Manager
- Setting an account password policy for IAM users
- Using multi-factor authentication (MFA) in AWS
- Configurazione dell'accesso multi-account con MFA
- Utilizzo di IAM Access Analyzer per creare policy IAM
- Best Practices for AWS Organizations Service Control Policies in a Multi-Account Environment
- How to Receive Notifications When Your AWS Account's Root Access Keys Are Used
- Create fine-grained session permissions using IAM managed policies
- Break glass access

Video correlati:

- Automating Incident Response and Forensics in AWS
- DIY guide to runbooks, incident reports, and incident response
- Prepare for and respond to security incidents in your AWS environment

SEC10-BP06 Implementazione anticipata degli strumenti

Verifica che il team addetto alla sicurezza disponga degli strumenti giusti pre-implementati per ridurre i tempi di indagine fino al ripristino.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all’implementazione

Per automatizzare le funzioni delle operazioni e la risposta di sicurezza, puoi utilizzare un set completo di API e strumenti AWS. Puoi automatizzare completamente le funzionalità di gestione delle identità, sicurezza della rete, protezione dei dati e monitoraggio e distribuirle utilizzando metodi di sviluppo software comuni già esistenti. Quando crei l’automazione della sicurezza, il sistema può monitorare, rivedere e avviare una risposta, anziché far sì che le persone monitorino la tua posizione di sicurezza e reagiscano manualmente agli eventi.

Se i team di risposta agli incidenti continuano a rispondere agli avvisi nello stesso modo, rischiano il cosiddetto affaticamento dagli avvisi ("alert fatigue"). Ciò significa che, nel corso del tempo, il team può diventare desensibilizzato agli avvisi e commettere errori nella gestione di situazioni ordinarie o farsi sfuggire avvisi insoliti. L’automazione aiuta a evitare l’affaticamento dagli avvisi mediante

funzioni che elaborano gli avvisi ripetitivi e ordinari, lasciando alle persone la gestione degli incidenti sensibili e univoci. L'integrazione di sistemi di rilevamento delle anomalie, come Amazon GuardDuty, AWS CloudTrail Insights e Amazon CloudWatch Anomaly Detection può ridurre l'impatto di avvisi frequenti basati su soglie.

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

Durante un'indagine di sicurezza, devi essere in grado di esaminare i log pertinenti per registrare e comprendere l'intera portata e la tempistica dell'incidente. I log servono anche per la generazione di avvisi, che indicano il verificarsi di determinate azioni di interesse. È fondamentale selezionare, attivare, memorizzare e impostare i meccanismi di query e recupero e impostare gli avvisi. Inoltre, una soluzione efficace per fornire gli strumenti di ricerca nei dati di log è Amazon Detective.

AWS offre oltre 200 servizi cloud e migliaia di funzionalità. Ti consigliamo di esaminare i servizi in grado di supportare e semplificare la tua strategia di risposta agli incidenti.

Oltre ai log, è necessario sviluppare e implementare una strategia di assegnazione tag. L'assegnazione dei tag può fornire il contesto per lo scopo di una risorsa AWS e può essere utilizzata anche per l'automazione.

Passaggi dell'implementazione

Seleziona e configura i log per analisi e avvisi

Consulta la seguente documentazione sulla configurazione dei log per la risposta agli incidenti:

- Logging strategies for security incident response
- SEC04-BP01 Configurazione dei log di servizi e applicazioni

Enable security services to support detection and response

AWS offre funzionalità investigative, preventive e reattive e altri servizi utilizzabili per progettare soluzioni di sicurezza personalizzate. Per un elenco dei servizi più pertinenti per la risposta agli incidenti di sicurezza, consulta Definizioni delle capacità del cloud e la Homepage della risposta agli incidenti di sicurezza.

Sviluppa e implementa una strategia di assegnazione tag

Ottenere informazioni contestuali sul caso d'uso aziendale e sulle parti interessante interne pertinenti relativi a una risorsa AWS può essere difficile. Un modo per farlo sono i tag che assegnano i metadati alle risorse AWS e sono composti da una chiave e un valore definiti dall'utente. Puoi creare i tag per classificare le risorse per scopo, proprietario, ambiente, tipo di dati elaborati e altri criteri di tua scelta.

Avere una strategia di assegnazione tag coerente può accelerare le risposta e ridurre al minimo il tempo dedicato al contesto organizzativo, consentendo di identificare e discernere rapidamente le informazioni contestuali su una risorsa AWS. I tag possono anche fungere da meccanismo per avviare le automazioni di risposta. Per maggiori dettagli su cosa taggare, consulta Taggare le risorse AWS. Dovrai prima definire i tag nella tua organizzazione e quindi implementare e applicare questa strategia di tag. Per maggiori dettagli su implementazione e applicazione, consulta Implement AWS resource tagging strategy using AWS Tag Policies and Service Control Policies (SCPs).

Risorse

Best practice Well-Architected correlate:

- SEC04-BP01 Configurazione dei log di servizi e applicazioni
- SEC04-BP02 Acquisizione di log, esiti e metriche in posizioni standardizzate

Documenti correlati:

- Logging strategies for security incident response
- Incident response cloud capability definitions

Esempi correlati:

- Threat Detection and Response with Amazon GuardDuty and Amazon Detective
- Workshop Security Hub
- Gestione delle vulnerabilità con Amazon Inspector

SEC10-BP07 Esecuzione di simulazioni

Man mano che le organizzazioni crescono e si evolvono nel tempo, aumentano anche le tipologie di minacce. Per questo motivo, è importante rivedere continuamente le capacità di risposta agli

incidenti. L'esecuzione di simulazioni (note anche come giornate di gioco) è un metodo che può essere utilizzato per eseguire questa valutazione. Le simulazioni utilizzano scenari di eventi di sicurezza reali progettati per simulare le tattiche, le tecniche e le procedure (TTP) di un autore di minacce e consentire a un'organizzazione di esercitarsi e valutare le proprie capacità di risposta agli incidenti rispondendo a questi finti eventi informatici così come potrebbero verificarsi nella realtà.

Vantaggi dell'adozione di questa best practice: le simulazioni offrono una serie di vantaggi.

- Convalida della preparazione informatica e sviluppo della fiducia dei team di risposta agli incidenti.
- Verifica della precisione e dell'efficienza di strumenti e flussi di lavoro.
- Perfezionamento dei metodi di comunicazione ed escalation in linea con il piano di risposta agli incidenti.
- Opportunità di rispondere per i vettori meno comuni.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

Esistono tre tipi principali di simulazioni:

- Simulazioni di situazioni di emergenza le simulazioni di situazioni di emergenza sono sessioni basate sulla discussione che coinvolgono le varie parti interessate alla risposta agli incidenti per mettere in pratica ruoli e responsabilità e utilizzare strumenti e playbook di comunicazione consolidati. Lo svolgimento dell'esercitazione può in genere essere eseguito in un'intera giornata in un luogo virtuale, in un luogo fisico o in una combinazione di questi tipi di luogo. Poiché è basato sulla discussione, questo tipo di esercitazione si concentra su processi, persone e collaborazione. La tecnologia è parte integrante della discussione, ma l'uso effettivo di strumenti o script di risposta agli incidenti in genere non rientra in questo tipo di simulazione.
- Esercitazioni con il team viola: questo tipo di esercitazioni aumenta il livello di collaborazione tra i team di risposta agli incidenti (team blu) e gli attori delle minacce simulate (team rosso). Il team blu è composto da membri del Security Operations Center (SOC), ma può includere anche altre parti interessate che sarebbero coinvolte durante un vero e proprio evento informatico. Il team rosso è composto da un team responsabile dei test di penetrazione o da parti interessate chiave esperte in materia di sicurezza informatica. Il team rosso lavora assieme ai coordinatori dell'esercitazione durante la progettazione di uno scenario in modo che questi sia accurato e fattibile. Durante le esercitazioni del team viola, l'attenzione è rivolta principalmente ai meccanismi di rilevamento, agli strumenti e alle procedure operative standard (SOP) a supporto della risposta agli incidenti.

- Esercitazioni con il team rosso: durante un'esercitazione con il team rosso, l'attacco (team rosso) effettua una simulazione per raggiungere un determinato obiettivo o una serie di obiettivi da un ambito predeterminato. I difensori (team blu) non saranno necessariamente a conoscenza della portata e della durata dell'esercitazione, il che fornisce una valutazione più realistica di come risponderebbero a un incidente reale. Poiché le esercitazioni con il team rosso possono basarsi su test invasivi, procedi con cautela e implementa controlli per verificare che l'esercitazione non causi danni effettivi all'ambiente.

Prendi in considerazione la possibilità di svolgere simulazioni informatiche a intervalli regolari. Ogni tipo di esercitazione può offrire vantaggi unici ai partecipanti e all'organizzazione nel suo insieme; potresti, quindi, scegliere di iniziare con tipi di simulazione meno complessi (come le simulazioni di situazioni di emergenza) e passare a tipi di simulazione più complessi (esercitazioni del team rosso). È necessario selezionare un tipo di simulazione in base alla maturità, alle risorse e ai risultati desiderati a livello di sicurezza. Alcuni clienti potrebbero scegliere di non eseguire le esercitazioni del team rosso a causa della loro complessità e dei loro costi.

Passaggi dell'implementazione

Indipendentemente dal tipo di simulazione scelto, le simulazioni sono in genere caratterizzate dai seguenti passaggi di implementazione:

1. Definisci gli elementi principali dell'esercitazione: definisci scenario e obiettivi della simulazione. Lo scenario e gli obiettivi dovrebbero essere entrambi accettati dalla leadership.
2. Identifica le parti interessate principali: come minimo, un'esercitazione prevede la presenza di coordinatori e partecipanti. A seconda dello scenario, potrebbero essere coinvolte altre parti interessate come la leadership legale, delle comunicazioni o esecutiva.
3. Crea ed esegui il test dello scenario: potrebbe essere necessario ridefinire lo scenario durante la creazione se risulta impossibile implementare elementi specifici. Come risultato di questa fase è previsto uno scenario definitivo.
4. Fai svolgere la simulazione: il tipo di simulazione determina il tipo di svolgimento usato (uno scenario basato su supporto cartaceo o uno scenario con simulazione altamente tecnologica). I coordinatori dovrebbero allineare le loro tattiche di svolgimento agli oggetti dell'esercitazione e dovrebbero coinvolgere tutti i partecipanti ove possibile per ottimizzare i benefici.
5. Predisponi il report post-azione (AAR): identifica le aree positive, quelle da migliorare e le potenziali lacune. Il report AAR dovrebbe misurare l'efficacia della simulazione e la risposta

del team all'evento simulato in modo che i progressi possano essere monitorati nel tempo con simulazioni future.

Risorse

Documenti correlati:

- Guida sulla risposta agli incidenti di sicurezza di AWS

Video correlati:

- AWS GameDay - Security Edition
- Esecuzione di simulazioni di risposta agli incidenti di sicurezza efficaci

Operazioni

Le operazioni sono il fulcro dell'esecuzione della risposta agli incidenti. È qui che avvengono le azioni di risposta e riparazione degli incidenti di sicurezza. Le operazioni comprendono le seguenti cinque fasi: rilevamento, analisi, contenimento, rimozione e ripristino. La descrizione di queste fasi e degli obiettivi è disponibile nella tabella seguente.

Fase	Obiettivo
Rilevamento	Identifica un potenziale evento di sicurezza.
Analisi	Determina se l'evento di sicurezza è un incidente e valutane la portata.
Contenimento	Riduci al minimo e limita l'ambito dell'evento di sicurezza.
Rimozione	Rimuovi risorse o artefatti non autorizzati correlati all'evento di sicurezza. Implementa le mitigazioni che hanno causato l'incidente di sicurezza.

Fase	Obiettivo
Ripristino	Ripristina i sistemi allo stato di sicurezza noto e monitorali per verificare che la minaccia non si ripresenti.

Queste fasi dovrebbero servire da guida quando si risponde e si opera sugli incidenti di sicurezza per garantire una risposta efficace e forte. Le azioni effettive che intraprenderai variano a seconda dell'incidente. Un incidente relativo a un ransomware, ad esempio, presenta una serie di passaggi di risposta diversi da quelli di un incidente che coinvolge un bucket Amazon S3 pubblico. Inoltre, questi passaggi non devono essere seguiti necessariamente in sequenza. Dopo il contenimento e la rimozione, potrebbe essere necessario tornare all'analisi per capire se le azioni intraprese sono state efficaci.

Una preparazione approfondita del personale, dei processi e della tecnologia è fondamentale per garantire operazioni efficaci. Pertanto, attieniti alle best practice di cui alla sezione Preparazione così da poter rispondere in modo efficace a un evento di sicurezza attivo.

Per ulteriori informazioni, consulta la sezione Operations della AWS Security Incident Response Guide.

Attività post-incidente

Il panorama delle minacce è in continua evoluzione ed è importante essere altrettanto dinamici in termini di capacità dell'organizzazione di proteggere efficacemente gli ambienti. La chiave per il miglioramento continuo è l'iterazione degli esiti degli incidenti e delle simulazioni per migliorare le capacità di rilevare, rispondere e indagare efficacemente su possibili incidenti di sicurezza, riducendo le possibili vulnerabilità, i tempi di risposta e ripristinando operazioni sicure. I seguenti meccanismi possono aiutarti a verificare che la tua organizzazione sia sempre preparata a rispondere efficacemente grazie alle funzionalità e alle conoscenze più recenti, indipendentemente dalla situazione.

Best practice

- SEC10-BP08 Definizione di un framework per apprendere dagli incidenti

SEC10-BP08 Definizione di un framework per apprendere dagli incidenti

L'implementazione di un framework basato sulle lezioni apprese e di una capacità di analisi delle cause principali non solo contribuisce a migliorare le capacità di risposta agli incidenti, ma aiuta anche a prevenire il ripetersi dell'incidente. Imparando da ogni incidente, puoi evitare di ripetere gli errori, i rischi o le configurazioni non valide, non solo migliorando il tuo livello di sicurezza, ma anche riducendo al minimo il tempo speso in situazioni evitabili.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all’implementazione

È importante implementare un framework basato sulle lezioni apprese in grado di stabilire e raggiungere, a un livello elevato, i seguenti punti:

- Quando si tiene un framework basato sulle lezioni apprese?
- Cosa comporta il processo basato sulle lezioni apprese?
- Come viene eseguito un framework basato sulle lezioni apprese?
- Chi è coinvolto nel processo e in che modo?
- Come vengono identificate le aree di miglioramento?
- In che modo garantisci che i miglioramenti vengano monitorati e implementati in modo efficace?

Il framework non deve concentrarsi sugli individui, ma sul miglioramento di strumenti e processi.

Passaggi dell'implementazione

A parte i risultati di alto livello sopra elencati, è importante porsi le domande giuste per trarre il massimo valore (informazioni che portano a miglioramenti attuabili) dal processo. Considera queste domande per iniziare a promuovere le discussioni sulle lezioni apprese:

- Qual è stato l'incidente?
- Quando è stato identificato per la prima volta l'incidente?
- Come è stato identificato?
- Quali sistemi hanno avvisato dell'attività?
- Quali sistemi, servizi e dati sono stati coinvolti?

- Cosa è successo nello specifico?
- Cosa ha funzionato bene?
- Cosa non ha funzionato bene?
- Quale processo o quali procedure non sono riusciti a scalare per rispondere all'incidente?
- Cosa può essere migliorato nelle seguenti aree:
  - Persone
    - Le persone da contattare erano effettivamente disponibili e l'elenco dei contatti era aggiornato?
    - Le persone presentavano lacune nella formazione o nelle capacità necessarie per rispondere e indagare efficacemente sull'incidente?
    - Le risorse appropriate erano pronte e disponibili?
  - Processo
    - Sono stati seguiti i processi e le procedure?
    - I processi e le procedure erano documentati e disponibili per questo tipo di incidente?
    - Mancavano i processi e le procedure richiesti?
    - Il team di risposta è stato in grado di accedere tempestivamente alle informazioni necessarie per rispondere al problema?
  - Tecnologia
    - I sistemi di avviso esistenti hanno identificato e segnalato efficacemente l'attività?
    - Come si sarebbe potuto ridurre il tempo di rilevamento del 50%?
    - Gli avvisi esistenti devono essere migliorati o è necessario creare nuovi avvisi per questo (tipo di) incidente?
    - Gli strumenti esistenti hanno consentito un'indagine efficace (ricerca/analisi) dell'incidente?
    - Cosa si può fare per identificare prima questo tipo di incidente?
    - Cosa si può fare per evitare che questo tipo di incidente si ripeta?
    - A chi appartiene il piano di miglioramento e come verifichi che sia stato implementato?
    - Qual è la tempistica per l'implementazione e il test del monitoraggio aggiuntivo o dei controlli e dei processi preventivi?

Questo elenco non è esaustivo, ma può fungere da punto di partenza per individuare quali sono le esigenze dell'organizzazione e dell'attività e come analizzarle per imparare in modo più efficace dagli incidenti e migliorare costantemente il proprio livello di sicurezza. La cosa più importante è iniziare

incorporando le lezioni apprese come parte standard del processo di risposta agli incidenti, della documentazione e delle aspettative di tutti le parti interessate.

Risorse

Documenti correlati:

- AWS Security Incident Response Guide - Establish a framework for learning from incidents
- NCSC CAF guidance - Lessons learned

Sicurezza delle applicazioni

Il termine sicurezza delle applicazioni (AppSec) descrive il processo complessivo di progettazione, creazione e test delle proprietà di sicurezza dei carichi di lavoro sviluppati. Devi individuare persone sufficientemente qualificate nell'organizzazione, comprendere le proprietà di sicurezza dell'infrastruttura di sviluppo e rilascio e usare l'automazione per identificare i problemi correlati alla sicurezza.

L'adozione di test della sicurezza delle applicazioni come componente regolare del ciclo di vita di sviluppo del software e dei processi successivi al rilascio ti fornisce un meccanismo strutturato per identificare, correggere e prevenire problemi di sicurezza delle applicazioni nell'ambiente di produzione.

La metodologia di sviluppo delle applicazioni deve includere controlli di sicurezza durante la progettazione, l'implementazione e il funzionamento dei carichi di lavoro. Nel frattempo, allinea il processo per una continua riduzione degli errori e l'azzeramento del debito tecnico. Ad esempio, usando la modellazione delle minacce durante la fase di progettazione, puoi individuare i difetti di progettazione e correggerli più facilmente e in modo meno costoso anziché attendere e mitigarli in un secondo momento.

Costi e complessità associati alla correzione dei difetti sono in genere inferiori nelle fasi iniziali del ciclo di vita di sviluppo del software. Il modo più semplice per risolvere i problemi è non averne affatto ed è per questo che un modello di rischio iniziale ti permette di concentrarti sui risultati corretti sin dalla fase di progettazione. Con l'evolvere del programma per la sicurezza delle applicazioni, puoi aumentare la quantità di test eseguiti tramite l'automazione, migliorare l'attendibilità del feedback degli sviluppatori e ridurre il tempo necessario per le revisioni della sicurezza. Tutte queste iniziative migliorano la qualità del software sviluppato e accelerano la distribuzione di funzionalità nell'ambiente di produzione.

Le presenti linee guida per l'implementazione si concentrano su quattro aree: organizzazione e cultura, sicurezza della pipeline, sicurezza nella pipeline e gestione delle dipendenze. Ciascuna area fornisce un set di principi che puoi applicare e una visione completa di come progettare, sviluppare, compilare, implementare ed eseguire carichi di lavoro.

AWS offre diversi approcci da usare per gestire il programma per la sicurezza delle applicazioni. Alcuni sono basati sulla tecnologia, mentre altri sono incentrati sulle persone e gli aspetti organizzativi del programma.

Best practice

- SEC11-BP01 Formazione per la sicurezza delle applicazioni
- SEC11-BP02 Automazione dei test lungo il ciclo di vita di sviluppo e test
- SEC11-BP03 Esecuzione di test di penetrazione a intervalli regolari
- SEC11-BP04 Esecuzione di revisioni del codice
- SEC11-BP05 Centralizzazione dei servizi per pacchetti e dipendenze
- SEC11-BP06 Implementazione programmatica del software
- SEC11-BP07 Valutazione regolare delle proprietà di sicurezza delle pipeline
- SEC11-BP08 Creazione di un programma per l'integrazione della titolarità della sicurezza nei team responsabili del carico di lavoro

SEC11-BP01 Formazione per la sicurezza delle applicazioni

Offri al tuo team una formazione su pratiche operative e di sviluppo sicure per consentire la creazione di software sicuro e di alta qualità. In questo modo, il team può a prevenire, rilevare e correggere i problemi di sicurezza nelle prime fasi del ciclo di vita dello sviluppo. Valuta la possibilità di fornire una formazione su modellazione delle minacce, pratiche di codifica sicure e utilizzo di servizi per configurazioni e operazioni sicure. Dai la possibilità al team di accedere alla formazione tramite risorse self-service e raccogli regolarmente i feedback per garantire un miglioramento continuo.

Risultato desiderato: il tuo team dispone delle conoscenze e delle competenze necessarie per progettare e creare software pensando alla sicurezza fin dal principio. Grazie alla formazione su modellazione delle minacce e pratiche di sviluppo sicure, il team ottiene una conoscenza approfondita dei potenziali rischi per la sicurezza e dei metodi per mitigarli durante il ciclo di vita dello sviluppo software (SDLC). Questo approccio proattivo alla sicurezza si integra nella cultura del tuo team e hai la possibilità di identificare e correggere tempestivamente potenziali problemi di sicurezza. Di conseguenza, il tuo team crea software e funzionalità sicuri e di alta qualità in modo più efficiente, accelerando così le tempistiche di consegna complessive. All'interno dell'organizzazione la cultura della sicurezza è collaborativa e inclusiva: la titolarità della sicurezza è condivisa tra tutti gli sviluppatori.

Anti-pattern comuni:

- Attendi una revisione della sicurezza e poi valuti le proprietà di sicurezza di un sistema.
- Assegni tutte le decisioni in materia di sicurezza a un team responsabile della sicurezza.

- Manca la comunicazione della correlazione tra le decisioni adottate durante il ciclo di vita dello sviluppo software e le aspettative o policy complessive dell'organizzazione.
- Svolgi il processo di revisione della sicurezza in una fase troppo tardiva.

Vantaggi dell'adozione di questa best practice:

- Migliore identificazione dei requisiti aziendali per la sicurezza all'inizio del ciclo di sviluppo.
- Capacità di identificare e correggere più rapidamente possibili problemi di sicurezza, per una distribuzione più rapida delle funzionalità.
- Migliore qualità del software e dei sistemi.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

Per creare software sicuro e di alta qualità, offri al tuo team una formazione sulle pratiche comuni per lo sviluppo e la gestione delle applicazioni in sicurezza. In questo modo, il team può a prevenire, rilevare e correggere i problemi di sicurezza nelle prime fasi del ciclo di vita dello sviluppo, accelerando così le tempistiche di consegna.

Per raggiungere questo obiettivo, valuta la possibilità di formare il tuo team sulla modellazione delle minacce utilizzando risorse AWS come il workshop sulla modellazione delle minacce. La modellazione delle minacce può aiutare il team a comprendere i potenziali rischi per la sicurezza e a progettare i sistemi tenendo conto della sicurezza fin dal principio. Inoltre, puoi fornire l'accesso alle risorse di formazione di AWS Training Certification, di settore o dei Partner AWS sulle pratiche di sviluppo sicure. Per maggiori dettagli su un approccio completo alla progettazione, allo sviluppo, alla protezione e alla gestione efficiente su larga scala, consulta AWS DevOps Guidance.

Definisci e comunica in modo chiaro il processo di revisione della sicurezza dell'organizzazione e descrivi le responsabilità del tuo team, del team addetto alla sicurezza e delle altre parti interessate Pubblica linee guida self-service, esempi di codice e modelli che mostrino come soddisfare i requisiti di sicurezza. Puoi utilizzare servizi AWS come AWS CloudFormation, AWS Cloud Development Kit (AWS CDK) (AWS CDK) Constructs e Catalogo dei servizi per fornire configurazioni sicure preapprovate e ridurre la necessità di configurazioni personalizzate.

Raccogli periodicamente dal tuo team feedback sull'esperienza con il processo di revisione della sicurezza e la formazione correlata, e usalo per ottenere un miglioramento continuo. Organizza

GameDay o campagne di bug bash per identificare e risolvere i problemi di sicurezza, rafforzando al contempo le competenze del tuo team.

Passaggi dell'implementazione

1. Identifica le esigenze di formazione: valuta l'attuale livello delle competenze e le lacune nelle conoscenze all'interno del team in materia di pratiche di sviluppo sicure attraverso sondaggi, revisioni del codice o discussioni con i membri del team.
2. Pianifica la formazione: in base alle esigenze identificate, crea un piano di formazione che copra argomenti rilevanti come modellazione delle minacce, pratiche di codifica sicure, test di sicurezza e pratiche di implementazione sicure. Utilizza risorse come il workshop sulla modellazione delle minacce e i programmi di formazione di AWS Training and Certification, di settore o dei Partner AWS.
3. Pianifica e offri corsi di formazione: pianifica sessioni di formazione o workshop periodici per il tuo team. Possono essere tenuti da un istruttore o personalizzati, a seconda delle preferenze e della disponibilità del team. Incoraggia lo svolgimento di esercizi ed esempi pratici per rafforzare l'apprendimento.
4. Definisci un processo di revisione della sicurezza: collabora con il tuo team addetto alla sicurezza e con le altre parti interessate per definire chiaramente il processo di revisione della sicurezza per le tue applicazioni. Documenta le responsabilità di ogni team o individuo coinvolto nel processo, inclusi i team addetti allo sviluppo e alla sicurezza e incluse eventuali altre parti interessate.
5. Crea risorse self-service: sviluppa linee guida self-service, esempi di codice e modelli che mostrino come soddisfare i requisiti di sicurezza dell'organizzazione. Valuta la possibilità di utilizzare servizi AWS come CloudFormation, AWS CDK Constructs e Catalogo dei servizi per fornire configurazioni sicure preapprovate e ridurre la necessità di configurazioni personalizzate.
6. Comunica e socializza: comunica in modo efficace al tuo team il processo di revisione della sicurezza e le risorse self-service disponibili. Conduci sessioni di formazione o workshop per far acquisire familiarità con queste risorse e per verificare che sappiano come usarle.
7. Raccogli i feedback e migliora i processi: raccogli periodicamente dal tuo team feedback sull'esperienza con il processo di revisione di sicurezza e la formazione correlata. Utilizza i feedback per identificare le aree di miglioramento e migliorare continuamente i materiali di formazione, le risorse self-service e il processo di revisione della sicurezza.
8. Svolgi esercizi di sicurezza: organizza GameDay o campagne di bug bash per identificare e risolvere i problemi di sicurezza all'interno delle applicazioni. Questi esercizi non solo aiutano a scoprire potenziali vulnerabilità, ma offrono anche opportunità pratiche di apprendimento per il team, volte a migliorare le competenze in materia di sviluppo e gestione in sicurezza.

9. Continua a imparare e migliorare: incoraggia il tuo team a rimanere aggiornato sulle pratiche, sugli strumenti e sulle tecniche di sviluppo in sicurezza più recenti. Rivedi e aggiorna regolarmente i materiali e le risorse di formazione per riflettere le best practice e il panorama della sicurezza in continua evoluzione.

Risorse

Best practice correlate:

- SEC11-BP08 Creazione di un programma per l'integrazione della titolarità della sicurezza nei team responsabili del carico di lavoro

Documenti correlati:

- AWS Training and Certification
- How to think about cloud security governance
- How to approach threat modeling
- Accelerating training – The AWS Skills Guild
- AWS DevOps Sagas

Video correlati:

- Proactive security: Considerations and approaches

Esempi correlati:

- Workshop on threat modeling
- Industry awareness for developers

Servizi correlati:

- AWS CloudFormation
- AWS Cloud Development Kit (AWS CDK) (AWS CDK) Costrutti di
- Service Catalog

SEC11-BP02 Automazione dei test lungo il ciclo di vita di sviluppo e test

Automatizza i test per le proprietà di sicurezza lungo il ciclo di vita di sviluppo e test. L'automazione semplifica l'identificazione coerente e ripetibile dei potenziali problemi nel software prima del rilascio, riducendo il rischio di riscontrare problemi di sicurezza nel software fornito.

Risultato desiderato: l'obiettivo dei test automatizzati è fornire una soluzione programmatica per l'individuazione di potenziali problemi nelle fasi iniziali e spesso durante l'intero ciclo di vita dello sviluppo. Automatizzando i test di regressione, puoi ripetere l'esecuzione di test funzionali e non funzionali per verificare che il software testato in precedenza continui ad avere le prestazioni previste dopo una modifica. Quando definisci test di unità di sicurezza per verificare la presenza di configurazioni errate comuni, come autorizzazioni non corrette o mancanti, puoi identificare e correggere i problemi all'inizio del processo di sviluppo.

Per l'automazione dei test vengono usati casi di test dedicati per la convalida delle applicazioni, in base ai requisiti e alle funzionalità desiderate. Il risultato dei test automatici è basato sul confronto dell'output del test generato con quello previsto, che accelera l'intero ciclo di vita dei test. Metodologie di test come i test di regressione e le suite di test di unità sono ideali per l'automazione. L'automazione dei test delle proprietà di sicurezza permette agli sviluppatori di ricevere in automatico feedback senza attendere una revisione della sicurezza. I test automatici sotto forma di analisi statica o dinamica del codice possono migliorare la qualità del codice e semplificare il rilevamento dei potenziali problemi software all'inizio del ciclo di vita di sviluppo.

Anti-pattern comuni:

- Mancata comunicazione dei casi di test e dei risultati dei test automatici.
- Esecuzione dei test solo immediatamente prima di un rilascio.
- Automazione dei casi di test con requisiti che cambiano spesso.
- Assenza di linee guida su come gestire i risultati dei test di sicurezza.

Vantaggi dell'adozione di questa best practice:

- Riduzione della dipendenza da valutazioni personali delle proprietà di sicurezza dei sistemi.
- Migliore coerenza grazie a esiti uniformi tra più flussi di lavoro.
- Minore probabilità di introdurre problemi di sicurezza nel software di produzione.

- Intervallo di tempo più breve tra l'individuazione e la correzione grazie all'identificazione più tempestiva dei problemi software.
- Maggiore visibilità su comportamenti sistematici o ripetuti tra più flussi di lavoro, utile per favorire miglioramenti in tutta l'organizzazione.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

Durante lo sviluppo del software, adotta diversi meccanismi di test in modo da avere la certezza di testare l'applicazione per requisiti funzionali, basati sulla logica di business, e non funzionali, incentrati sull'affidabilità, sulle prestazioni e sulla sicurezza dell'applicazione.

I test di sicurezza statici dell'applicazione analizzano il codice sorgente in cerca di modelli di sicurezza anomali e forniscono indicazioni su un codice soggetto a errori. I test di sicurezza statici dell'applicazione si basano su input statici, come la documentazione (definizione dei requisiti, documentazione sulla progettazione e specifiche di progettazione) e il codice sorgente dell'applicazione, per testare un'ampia gamma di problemi di sicurezza noti. Gli analizzatori di codice statici possono contribuire ad accelerare l'analisi di volumi elevati di codice. Il NIST Quality Group fornisce un confronto tra gli analizzatori della sicurezza del codice sorgente, che include strumenti open source per la scansione del codice byte e la scansione del codice binario.

Integra i test statici con metodologie di test della sicurezza tramite analisi dinamica, che eseguono test sull'applicazione in esecuzione per identificare potenziali comportamenti imprevisti. I test dinamici consentono di individuare potenziali problemi non rilevabili tramite l'analisi statica. L'esecuzione di test nelle fasi di repository, compilazione e pipeline del codice permette di verificare potenziali problemi di tipi diversi, evitandone la presenza nel codice. Amazon Q Developer fornisce suggerimenti sul codice, tra cui la scansione di sicurezza, nell'ambiente IDE del generatore. La Sicurezza di Amazon CodeGuru è in grado di identificare problemi critici, problemi di sicurezza e bug difficili da individuare durante lo sviluppo di applicazioni e fornisce consigli per migliorare la qualità del codice. L'estrazione di documenti SBOM (Software Bill of Material) consente anche di estrarre un record formale contenente i dettagli e le relazioni dei vari componenti utilizzati nella creazione del software. Ciò consente di gestire le vulnerabilità in modo informato e di identificare rapidamente le dipendenze tra software o componenti e i rischi legati alla catena di approvvigionamento.

Il workshop Security for Developers utilizza strumenti AWS per gli sviluppatori, come AWS CodeBuild, AWS CodeCommit e AWS CodePipeline, per l'automazione della pipeline di rilascio che comprendono metodologie di test SAST e DAST.

Lungo il ciclo di vita di sviluppo del software definisci un processo iterativo che includa revisioni periodiche dell'applicazione con il team responsabile della sicurezza. Il feedback raccolto da queste revisioni della sicurezza deve essere affrontato e convalidato come parte della revisione dell'idoneità per il rilascio. Queste revisioni permettono di stabilire una solida posizione di sicurezza per l'applicazione e forniscono agli sviluppatori feedback di utilità pratica per affrontare i potenziali problemi.

Passaggi dell'implementazione

- Implementa un ambiente IDE, una revisione del codice e strumenti CI/CD coerenti che includano test di sicurezza.
- Determina le fasi del ciclo di vita di sviluppo del software in cui è opportuno bloccare le pipeline anziché informare semplicemente gli sviluppatori riguardo alla necessità di risolvere i problemi.
- Automated Security Helper (ASH) è un esempio di strumento di scansione open source che aiuta a verificare la sicurezza del codice.
- L'esecuzione di test o analisi del codice mediante strumenti automatizzati, come Amazon Q Developer, integrato con gli ambienti IDE per sviluppatori, e la Sicurezza di Amazon CodeGuru per la scansione del codice al momento del commit, consente agli sviluppatori di ricevere feedback al momento giusto.
- Se sviluppi usando AWS Lambda, puoi sfruttare Amazon Inspector per la scansione del codice dell'applicazione nelle tue funzioni.
- Se le pipeline CI/CD includono test automatici, devi usare un sistema di gestione dei ticket per tenere traccia della notifica e della correzione dei problemi software.
- Per test di sicurezza che possono generare esiti, il collegamento a linee guida per la correzione permette agli sviluppatori di migliorare la qualità del codice.
- Analizza regolarmente gli esiti ottenuti dagli strumenti automatici per definire le priorità delle successive iniziative di automazione, formazione degli sviluppatori o creazione di campagne di sensibilizzazione.
- Per estrarre documenti SBOM nell'ambito delle pipeline CI/CD, usa Amazon Inspector SBOM Generator per creare SBOM per archivi, immagini di container, directory, sistemi locali e binari Go e Rust compilati nel formato CycloneDX SBOM.

Risorse

Best practice correlate:

- DevOps Guidance: DL.CR.3 Establish clear completion criteria for code tasks

Documenti correlati:

- Distribuzione e implementazione continue

- AWS Partner con competenze in DevOps
- AWS Security Competency Partners per la sicurezza delle applicazioni
- Choosing a Well-Architected CI/CD approach
- Secrets detection in Amazon CodeGuru Security
- Amazon CodeGuru Security Detection Library
- Accelerate deployments on AWS with effective governance
- How AWS approaches automating safe, hands-off deployments
- How Amazon CodeGuru Security helps you effectively balance security and velocity

Video correlati:

- Hands-off: Automating continuous delivery pipelines at Amazon
- Automating cross-account CI/CD pipelines
- The Software Development Process at Amazon
- Testing software and systems at Amazon

Esempi correlati:

- Industry awareness for developers
- Automated Security Helper (ASH)
- AWS CodePipeline Governance - Github

SEC11-BP03 Esecuzione di test di penetrazione a intervalli regolari

Esegui regolarmente test di penetrazione sul software. Questo meccanismo ti consente di identificare potenziali problemi relativi al software che non possono essere rilevati dai test automatizzati o dalla revisione manuale del codice e può anche aiutarti a capire l'efficacia dei tuoi controlli di rilevamento.

I test di penetrazione devono determinare se il software può essere reso operativo in modi imprevisti, ad esempio esponendo dati che da proteggere o concedendo autorizzazioni più elevate del previsto.

Risultato desiderato: utilizzo del test di penetrazione per rilevare, correggere e convalidare le proprietà di sicurezza dell'applicazione. È necessario eseguire test di penetrazione regolari e pianificati nell'ambito del ciclo di vita di sviluppo del software. Gli esiti ottenuti dai test di penetrazione devono essere gestiti prima del rilascio del software. Devi analizzare gli esiti dei test di penetrazione per identificare l'eventuale presenza di problemi identificabili con l'automazione. Un processo di esecuzione di test di penetrazione regolare e ripetibile, con un meccanismo di feedback attivo, aiuta a stabilire linee guida per gli sviluppatori e migliora la qualità del software.

Anti-pattern comuni:

- Esecuzione di test di penetrazione solo per problemi di sicurezza noti o comuni.
- Esecuzione di test di penetrazione delle applicazioni senza gli strumenti e le librerie di terze parti dipendenti.
- Esecuzione di test di penetrazione solo per i problemi di sicurezza relativi ai pacchetti, senza valutare la logica di business implementata.

Vantaggi dell'adozione di questa best practice:

- Maggiore certezza riguardo alle proprietà di sicurezza del software prima del rilascio.
- Opportunità di identificare i modelli comportamentali preferiti delle applicazioni, per una migliore qualità del software.
- Presenza di un ciclo di feedback che identifica all'inizio del ciclo di sviluppo i punti in cui l'automazione o una formazione aggiuntiva possono migliorare le proprietà di sicurezza del software.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

I test di penetrazione sono un esercizio strutturato per l'esecuzione di test di sicurezza in cui vengono eseguiti scenari di violazione della sicurezza pianificati per rilevare, correggere e convalidare i controlli di sicurezza. I test di penetrazione partono dalla ricognizione, durante la quale si raccolgono dati in base all'attuale progettazione dell'applicazione e alle sue dipendenze. Viene creato ed

eseguito un elenco selezionato di scenari di test specifici per la sicurezza. Lo scopo principale di questi test è rivelare i problemi di sicurezza nell'applicazione che potrebbero essere sfruttati per ottenere l'accesso indesiderato all'ambiente o l'accesso non autorizzato ai dati. Devi eseguire test di penetrazione quando lanci nuove funzionalità o ogni volta che l'applicazione viene sottoposta a modifiche importanti durante l'implementazione tecnica o di funzioni.

Devi identificare la fase più appropriata del ciclo di vita di sviluppo in cui eseguire i test di penetrazione. Questi test devono essere eseguiti nelle fasi finali, in modo che la funzionalità del sistema sia vicina allo stato di rilascio previsto, ma con tempo sufficiente per la correzione di eventuali problemi.

Passaggi dell'implementazione

- Adotta un processo strutturato per definire l'ambito dei test di penetrazione. Basare il processo sul modello di minaccia costituisce una buona soluzione per mantenere il contesto.
- Identifica la fase più appropriata del ciclo di vita di sviluppo in cui eseguire test di penetrazione. Questi devono avvenire quando sono previste modifiche minime nell'applicazione, ma quando vi è ancora tempo sufficiente per apportare eventuali correzioni.
- Prepara gli sviluppatori su cosa aspettarsi dagli esiti dei test di penetrazione e su come ottenere informazioni sulla correzione.
- Usa strumenti per accelerare il processo di esecuzione dei test di penetrazione automatizzando test comuni o ripetibili.
- Analizza gli esiti dei test di penetrazione per identificare problemi di sicurezza sistematici e usa questi dati per definire altri test automatici e formazione continua per gli sviluppatori.

Risorse

Best practice correlate:

- SEC11-BP01 Formazione per la sicurezza delle applicazioni
- SEC11-BP02 Automazione dei test lungo il ciclo di vita di sviluppo e test

Documenti correlati:

- La pagina relativa ai test di penetrazione AWS fornisce una guida dettagliata per i test di penetrazione su AWS

- Accelerate deployments on AWS with effective governance
- AWS Security Competency Partners
- Modernize your penetration testing architecture on AWS Fargate
- AWS Fault Injection Simulator

Esempi correlati:

- Automazione dei test API con AWS CodePipeline (GitHub)
- Helper di sicurezza automatizzato (GitHub)

SEC11-BP04 Esecuzione di revisioni del codice

Implementa le revisioni del codice per verificare la qualità e la sicurezza del software in fase di sviluppo. Le revisioni del codice prevedono che membri del team diversi da quelli che hanno originariamente scritto il codice esaminino il codice stesso per individuare potenziali problemi e vulnerabilità e l'aderenza agli standard e alle best practice in materia di codifica. Questo processo aiuta a individuare errori, incongruenze e difetti di sicurezza che potrebbero essere stati trascurati dallo sviluppatore originale. Utilizza strumenti automatici per facilitare la revisione del codice.

Risultato desiderato: le revisioni del codice vengono incluse durante la fase di sviluppo per aumentare la qualità del software in fase di scrittura. Le competenze dei membri meno esperti del team migliorano grazie ad apprendimenti identificati durante la revisione del codice. Vengono identificate le opportunità di automazione e il processo di revisione del codice viene supportato con strumenti e test automatizzati.

Anti-pattern comuni:

- Il codice non viene revisionato prima dell'implementazione.
- Scrittura e revisione del codice effettuate dalla stessa persona.
- Mancato utilizzo dell'automazione e degli strumenti per facilitare o orchestrare le revisioni del codice.
- Mancata formazione degli sviluppatori sulla sicurezza dell'applicazione prima di eseguire la revisione del codice.

Vantaggi dell'adozione di questa best practice:

- Migliore qualità del codice.
- Maggiore coerenza dello sviluppo del codice attraverso il riutilizzo di approcci comuni.
- Riduzione del numero di problemi riscontrati durante i test di penetrazione e nelle fasi successive.
- Migliore circolazione delle informazioni all'interno del team.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

Le revisioni del codice aiutano a verificare la qualità e la sicurezza del software durante la fase di sviluppo. Le revisioni manuali prevedono che membri del team diversi da quelli che hanno originariamente scritto il codice esaminino il codice stesso per individuare potenziali problemi e vulnerabilità e l'aderenza agli standard e alle best practice in materia di codifica. Questo processo aiuta a individuare errori, incongruenze e difetti di sicurezza che potrebbero essere stati trascurati dallo sviluppatore originale.

Valuta la possibilità di utilizzare Sicurezza di Amazon CodeGuru per condurre revisioni automatiche del codice. Sicurezza di CodeGuru utilizza il machine learning e il ragionamento automatico per analizzare il codice e identificare potenziali vulnerabilità di sicurezza e problemi di codifica. Integra le revisioni automatiche del codice con i repository di codice e le pipeline di integrazione continua/distribuzione continua (CI/CD) esistenti.

Passaggi dell'implementazione

1. Stabilisci un processo di revisione del codice:
   - Definisci quando devono essere eseguite le revisioni del codice, ad esempio prima di unire il codice nel ramo principale o prima dell'implementazione in produzione.
   - Determina chi deve essere coinvolto nel processo di revisione del codice, ad esempio i membri del team, gli sviluppatori senior e gli esperti di sicurezza.
   - Decidi la metodologia di revisione del codice, inclusi il processo e gli strumenti da utilizzare.
2. Configura gli strumenti di revisione del codice:
   - Valuta e seleziona gli strumenti di revisione del codice più adatti alle esigenze del tuo team, come le richieste pull di GitHub o Sicurezza di CodeGuru.
   - Integra gli strumenti scelti con i tuoi repository di codice e le pipeline CI/CD esistenti.
   - Configura gli strumenti per applicare i requisiti di revisione del codice, come il numero minimo di revisori e le regole di approvazione.

3. Definisci checklist e linee guida per la revisione del codice:
    - Crea una checklist o elabora delle linee guida per la revisione del codice che descrivano gli elementi da esaminare. Prendi in considerazione fattori come la qualità del codice, le vulnerabilità di sicurezza, l'aderenza agli standard di codifica e le prestazioni.
    - Condividi la checklist o le linee guida con il team di sviluppo e verifica che tutti comprendano le aspettative.
4. Forma gli sviluppatori sulle best practice per la revisione del codice:
    - Offri una formazione al tuo team su come condurre revisioni del codice efficaci.
    - Educa il team in merito ai principi di sicurezza delle applicazioni e alle vulnerabilità comuni da individuare durante le revisioni.
    - Incoraggia la condivisione delle conoscenze e abbina sessioni di programmazione per migliorare le competenze dei membri del team meno esperti.
5. Implementa il processo di revisione del codice:
    - Integra la fase di revisione del codice nel flusso di lavoro di sviluppo, ad esempio creando una richiesta pull e assegnando i revisori.
    - Richiedi che le modifiche al codice siano sottoposte a una revisione del codice prima dell'unione o dell'implementazione.
    - Incoraggia una comunicazione aperta e la comunicazione di feedback costruttivi durante il processo di revisione.
6. Monitora e migliora i processi:
    - Verifica regolarmente l'efficacia del processo di revisione del codice e raccogli feedback dal team.
    - Identifica le opportunità di automazione o di miglioramento degli strumenti per semplificare il processo di revisione del codice.
    - Aggiorna e perfeziona continuamente la checklist o le linee guida per la revisione del codice in base agli apprendimenti e alle best practice di settore.
7. Sensibilizza sull'importanza della revisione del codice:
    - Sottolinea l'importanza delle revisioni del codice per mantenere la qualità e la sicurezza del codice a un livello elevato.
    - Celebra i successi e gli apprendimenti frutto del processo di revisione del codice.
    - Incoraggia lo sviluppo di un ambiente collaborativo e di supporto in cui gli sviluppatori si sentano a proprio agio nel fornire e ricevere feedback.

Risorse

Best practice correlate:

- SEC11-BP02 Automazione dei test lungo il ciclo di vita di sviluppo e test

Documenti correlati:

- DevOps Guidance: DL.CR.2 Perform peer review for code changes
- About pull requests in GitHub

Esempi correlati:

- Automate code reviews with Amazon CodeGuru Security
- Automating detection of security vulnerabilities and bugs in CI/CD pipelines using Amazon CodeGuru Security CLI

Video correlati:

- Continuous improvement of code quality with Amazon CodeGuru Security

SEC11-BP05 Centralizzazione dei servizi per pacchetti e dipendenze

Fornisci servizi centralizzati per permettere ai tuoi team di ottenere pacchetti software e altre dipendenze. Questo approccio permette la convalida dei pacchetti prima di includerli nel software scritto e fornisce un'origine dati per l'analisi del software usato nell'organizzazione.

Risultato desiderato: il carico di lavoro viene creato sulla base di pacchetti software esterni in aggiunta al codice scritto dal tuo team. In questo modo, è più facile implementare funzionalità usate ripetutamente, come un parser JSON o una libreria di crittografia. Le origini per tali pacchetti e dipendenze vengono centralizzate, così che il tuo team addetto alla sicurezza possa convalidarle prima che vengano utilizzate. Questo approccio viene utilizzato insieme ai flussi di test manuali e automatici per garantire ulteriormente la qualità del software sviluppato.

Anti-pattern comuni:

- Recupero di pacchetti da repository arbitrari su Internet.
- Mancata esecuzione di test sui nuovi pacchetti prima di renderli disponibili agli sviluppatori.

Vantaggi dell'adozione di questa best practice:

- Migliore comprensione dei pacchetti usati nel software sviluppato.
- Capacità di informare i team responsabili del carico di lavoro quando un pacchetto deve essere aggiornato in base alle informazioni su chi usa cosa.
- Minor rischio di includere nel software un pacchetto con problemi.

Livello di rischio associato se questa best practice non fosse adottata: medio

Guida all'implementazione

Fornisci servizi centralizzati per i pacchetti e le dipendenze in modo da semplificarne l'uso per gli sviluppatori. La centralizzazione dei servizi può essere eseguita in modo logico anziché implementarli come sistema monolitico. Questo approccio permette di fornire servizi in modo da soddisfare le esigenze degli sviluppatori. Devi implementare una soluzione ottimale per l'aggiunta di pacchetti al repository in caso di aggiornamenti o nuovi requisiti. Servizi AWS come AWS CodeArtifact o soluzioni simili dei partner AWS forniscono tale funzionalità.

Passaggi dell'implementazione

- Implementa un servizio di repository centralizzato in modo logico che sia disponibile in tutti gli ambienti in cui viene sviluppato il software.
- Includi l'accesso al repository come parte del processo di provisioning automatico dell'Account AWS.
- Crea automazione per testare i pacchetti prima della loro pubblicazione in un repository.
- Gestisci le metriche dei pacchetti, dei linguaggi e dei team usati più comunemente e con la maggiore quantità di modifiche.
- Offri ai team di sviluppo un meccanismo automatico per richiedere nuovi pacchetti e fornire feedback.
- Analizza regolarmente i pacchetti nel repository per identificare il possibile impatto di nuovi problemi riscontrati.

Risorse

Best practice correlate:

- SEC11-BP02 Automazione dei test lungo il ciclo di vita di sviluppo e test

Documenti correlati:

- DevOps Guidance: DL.CS.2 Sign code artifacts after each build
- Supply chain Levels for Software Artifacts (SLSA)

Esempi correlati:

- Accelerate deployments on AWS with effective governance
- Tighten your package security with CodeArtifact Package Origin Control toolkit
- Multi Region Package Publishing Pipeline (GitHub)
- Publishing Node.js Modules on AWS CodeArtifact using AWS CodePipeline (GitHub)
- AWS CDK Java CodeArtifact Pipeline Sample (GitHub)
- Distribute private .NET NuGet packages with AWS CodeArtifact (GitHub)

Video correlati:

- Proactive security: Considerations and approaches
- The AWS Philosophy of Security (re:Invent 2017)
- When security, safety, and urgency all matter: Handling Log4Shell

SEC11-BP06 Implementazione programmatica del software

Esegui implementazioni programmatiche del software laddove possibile. Questo approccio riduce la probabilità che un'implementazione non riesca o che si verifichi un problema imprevisto a causa dell'errore umano.

Risultato desiderato: la versione del carico di lavoro da testare è la stessa che viene implementata e l'implementazione viene eseguita in modo coerente ogni volta. L'esternalizzazione della configurazione del carico di lavoro è utile per eseguirne l'implementazione in ambienti diversi senza

modifiche. Viene utilizzata la firma crittografica dei pacchetti software per verificare che non vi siano cambiamenti da un ambiente all'altro.

Anti-pattern comuni:

- Implementazione manuale del software nell'ambiente di produzione.
- Applicazione manuale di modifiche al software per soddisfare i requisiti di ambienti diversi.

Vantaggi dell'adozione di questa best practice:

- Maggiore affidabilità del processo di rilascio del software.
- Riduzione dei rischi legati a modifiche errate che hanno impatto sulla funzionalità aziendale.
- Processi di rilascio più frequenti grazie a un rischio di modifica minimo.
- Funzionalità di rollback automatiche in caso di eventi imprevisti durante l'implementazione.
- Possibilità di usare la crittografia per dimostrare che il software implementato è esattamente identico a quello testato.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Per mantenere un'infrastruttura applicativa solida e affidabile, implementa pratiche per l'implementazione sicura e automatizzata. Tali pratiche prevedono la rimozione dell'accesso umano persistente dagli ambienti di produzione, l'utilizzo di strumenti CI/CD per le implementazioni e l'esternalizzazione dei dati di configurazione specifici dell'ambiente. Seguendo questo approccio, è possibile migliorare la sicurezza, ridurre il rischio di errori umani e semplificare il processo di implementazione.

È possibile creare una struttura di Account AWS per rimuovere l'accesso umano persistente dagli ambienti di produzione. Questa pratica riduce al minimo il rischio di modifiche non autorizzate o accidentali, migliorando l'integrità dei sistemi di produzione. Invece dell'accesso umano diretto, puoi utilizzare strumenti CI/CD come AWS CodeBuild e AWS CodePipeline per eseguire le implementazioni. È possibile utilizzare questi servizi per automatizzare i processi di sviluppo, test e implementazione, riducendo l'intervento manuale e aumentando la coerenza.

Per migliorare ulteriormente la sicurezza e la tracciabilità, puoi firmare i pacchetti applicativi dopo che sono stati testati e convalidare le firme durante l'implementazione. A tale scopo, puoi usare strumenti

crittografici come AWS Signer o AWS Key Management Service (AWS KMS). Firmando e verificando i pacchetti, puoi assicurarti di distribuire solo codice autorizzato e convalidato nei tuoi ambienti.

Inoltre, il tuo team può progettare il carico di lavoro per ottenere dati di configurazione specifici dell'ambiente da una fonte esterna, come AWS Systems Manager Parameter Store. Questa pratica separa il codice dell'applicazione dai dati di configurazione, il che consente di gestire e aggiornare le configurazioni in modo indipendente senza modificare il codice applicativo stesso.

Per semplificare il provisioning e la gestione dell'infrastruttura, valuta la possibilità di utilizzare strumenti di infrastructure as code (IaC) come AWS CloudFormation o AWS CDK. Puoi utilizzare questi strumenti per definire l'infrastruttura come codice, con conseguente miglioramento della coerenza e della ripetibilità delle implementazioni in ambienti diversi.

Prendi in considerazione le distribuzioni canary per convalidare la corretta implementazione del tuo software. Le distribuzioni canary prevedono l'implementazione delle modifiche in un sottoinsieme di istanze o utenti prima dell'implementazione nell'intero ambiente di produzione. È quindi possibile monitorare l'impatto delle modifiche ed eventualmente annullarle, se necessario, in modo da ridurre al minimo il rischio di problemi diffusi.

Segui i consigli delineati nel white paper Organization Your AWS Environment Using Multiple Accounts. Questo white paper fornisce indicazioni su come suddividere gli ambienti (ad esempio, tra ambiente di sviluppo, di gestione temporanea e di produzione) in Account AWS distinti, con conseguente ulteriore miglioramento della sicurezza e dell'isolamento.

Passaggi dell'implementazione

1. Configurazione della struttura di Account AWS:
   - Segui le indicazioni contenute nel white paper Organization Your AWS Environment Using Multiple Accounts per creare Account AWS separati per ambienti diversi (ad esempio, ambiente di sviluppo, di gestione temporanea e di produzione).
   - Configura le autorizzazioni e i controlli di accesso appropriati per ogni account per limitare l'accesso umano diretto agli ambienti di produzione.
2. Implementa una pipeline CI/CD:
   - Configura una pipeline CI/CD utilizzando servizi come AWS CodeBuild e AWS CodePipeline.
   - Configura la pipeline per creare, testare e implementare automaticamente il codice applicativo nei rispettivi ambienti.
   - Integra i repository di codice con la pipeline CI/CD per il controllo delle versioni e la gestione del codice.

3. Firma e verifica i pacchetti applicativi:
   - Usa AWS Signer o AWS Key Management Service (AWS KMS) per firmare i pacchetti applicativi dopo che sono stati testati e convalidati.
   - Configura il processo di implementazione per verificare le firme dei pacchetti applicativi prima di distribuirli negli ambienti di destinazione.
4. Esternalizza i dati di configurazione:
   - Archivia i dati di configurazione specifici dell'ambiente in AWS Systems Manager Parameter Store.
   - Modifica il codice applicativo per recuperare i dati di configurazione dal Parameter Store durante l'implementazione o il runtime.
5. Implementa l'infrastructure as code (IaC):
   - Usa strumenti IaC come AWS CloudFormation o AWS CDK per definire e gestire la tua infrastruttura come codice.
   - Crea modelli CloudFormation o script CDK per fornire e configurare le risorse AWS necessarie per la tua applicazione.
   - Integra l'IaC con la tua pipeline CI/CD per implementare automaticamente le modifiche all'infrastruttura insieme alle modifiche al codice applicativo.
6. Implementa la distribuzione canary:
   - Configura il processo di implementazione per supportare le distribuzioni canary, in cui le modifiche vengono implementate in un sottoinsieme di istanze o utenti prima dell'implementazione nell'intero ambiente di produzione.
   - Utilizza servizi come AWS CodeDeploy o AWS ECS per gestire le distribuzioni canary e monitorare l'impatto delle modifiche.
   - Implementa meccanismi di rollback per tornare alla precedente versione stabile qualora vengano rilevati problemi durante la distribuzione canary.
7. Monitora ed esegui audit:
   - Configura meccanismi di monitoraggio e registrazione di log per tenere traccia delle implementazioni, delle prestazioni delle applicazioni e delle modifiche all'infrastruttura.
   - Usa servizi come Amazon CloudWatch e AWS CloudTrail per raccogliere e analizzare log e metriche.
   - Implementa controlli di conformità e audit per verificare l'aderenza alle best practice e ai requisiti normativi in materia di sicurezza.
8. Migliora continuamente i processi:

- Rivedi e aggiorna regolarmente le tue pratiche di implementazione, integrando feedback e informazioni apprese dalle implementazioni precedenti.
- Automatizza il più possibile il processo di implementazione per ridurre l'intervento manuale e i potenziali errori umani.
- Collabora con team interfunzionali (ad esempio, operativi o di sicurezza) per allineare e migliorare continuamente le pratiche di implementazione.

Seguendo questi passaggi, puoi mettere in atto pratiche di implementazione sicure e automatizzate nel tuo ambiente AWS, migliorando la sicurezza, riducendo il rischio di errori umani e semplificando il processo di implementazione.

Risorse

Best practice correlate:

- SEC11-BP02 Automazione dei test lungo il ciclo di vita di sviluppo e test
- DL.CI.2 Trigger builds automatically upon source code modifications

Documenti correlati:

- Accelerate deployments on AWS with effective governance
- Automatizzazione di distribuzioni pratiche e sicure
- Code signing using AWS Certificate Manager Private CA and AWS Key Management Service asymmetric keys
- Code Signing, a Trust and Integrity Control for AWS Lambda

Video correlati:

- Hands-off: Automating continuous delivery pipelines at Amazon

Esempi correlati:

- Blue/Green deployments with AWS Fargate

SEC11-BP07 Valutazione regolare delle proprietà di sicurezza delle pipeline

Applica i principi del pilastro della sicurezza Well-Architected alle pipeline, con particolare attenzione alla separazione delle autorizzazioni. Valuta regolarmente le proprietà di sicurezza della tua infrastruttura di pipeline. Una gestione efficace della sicurezza delle pipeline assicura la protezione del software che passa attraverso le pipeline.

Risultato desiderato: le pipeline in uso per la creazione e implementazione del tuo software seguono le stesse pratiche consigliate applicate per qualsiasi altro carico di lavoro nel tuo ambiente. I test che vengono implementati nelle pipeline non sono modificabili dai team che li utilizzano. Alle pipeline vengono assegnate solo le autorizzazioni necessarie per le implementazioni in esecuzione utilizzando credenziali temporanee. Vengono implementate misure di sicurezza per impedire che le pipeline vengano implementate negli ambienti sbagliati. Le pipeline vengono configurate in modo da comunicare lo stato, così da consentire la convalida dell'integrità degli ambienti di sviluppo.

Anti-pattern comuni:

- Test di sicurezza ignorabili dagli sviluppatori.
- Autorizzazioni eccessivamente elevate per le pipeline di implementazione.
- Pipeline non configurate per la convalida degli input.
- Nessuna revisione periodica delle autorizzazioni associate all'infrastruttura CI/CD.
- Uso di credenziali a lungo termine o hardcoded.

Vantaggi dell'adozione di questa best practice:

- Maggiore garanzia di integrità del software sviluppato e implementato attraverso le pipeline.
- Possibilità di arrestare un'implementazione in caso di attività sospetta.

Livello di rischio associato se questa best practice non fosse adottata: elevato

Guida all'implementazione

Le pipeline di implementazione sono una componente fondamentale del ciclo di vita dello sviluppo del software e devono seguire gli stessi principi e le stesse pratiche di sicurezza di qualsiasi altro carico di lavoro nel tuo ambiente. Ciò include l'implementazione di controlli di accesso adeguati, la convalida

degli input, oltre alla revisione e all'audit periodici delle autorizzazioni associate all'infrastruttura CI/CD.

Verifica che i team responsabili della creazione e della distribuzione delle applicazioni non siano in grado di modificare o aggirare i test e i controlli di sicurezza implementati nelle pipeline. Questa separazione delle responsabilità aiuta a mantenere l'integrità dei processi di creazione e implementazione.

Come punto di partenza, valuta la possibilità di utilizzare l'architettura AWS di riferimento per le pipeline di implementazione. Questa architettura di riferimento offre una base sicura e scalabile per la creazione di pipeline CI/CD su AWS.

Inoltre, è possibile utilizzare servizi come AWS Identity and Access Management Access Analyzer per generare policy IAM con privilegio minimo sia per le autorizzazioni delle pipeline sia per l'esecuzione di una fase delle pipeline destinata a verificare le autorizzazioni dei carichi di lavoro. Tutto questo consente di verificare che le pipeline e i carichi di lavoro dispongano solo delle autorizzazioni necessarie per le rispettive funzioni specifiche, riducendo il rischio di azioni o accessi non autorizzati.

Passaggi dell'implementazione

- Parti dall'architettura di riferimento per le pipeline di implementazione AWS.
- Prendi in considerazione l'utilizzo di AWS IAM Access Analyzer per generare in modo programmatico policy IAM con privilegio minimo per le pipeline.
- Integra nelle tue pipeline monitoraggio e avvisi in modo da ricevere notifiche in caso di attività impreviste o anomale, per i servizi AWS gestiti. Amazon EventBridge ti consente di indirizzare i dati verso destinazioni come AWS Lambda o Amazon Simple Notification Service (Amazon SNS).

Risorse

Documenti correlati:

- AWS Architettura di riferimento per pipeline di implementazione
- Monitoraggio di AWS CodePipeline
- Best practice di sicurezza per AWS CodePipeline

Esempi correlati:

- DevOps monitoring dashboard (GitHub)

SEC11-BP08 Creazione di un programma per l'integrazione della titolarità della sicurezza nei team responsabili del carico di lavoro

Crea un programma o un meccanismo che permetta ai team di sviluppo di prendere decisioni sulla sicurezza del software che creano. Il team della sicurezza dovrà convalidare queste decisioni durante una revisione, ma integrare la proprietà della sicurezza nei team di sviluppo consente di creare carichi di lavoro più veloci e sicuri. Questo meccanismo promuove anche una cultura della responsabilità che ha un impatto positivo sul funzionamento dei sistemi che crei.

Risultato desiderato: integrazione della titolarità della sicurezza e dei processi decisionali correlati nei team. I tuoi team hanno ricevuto una formazione sul corretto approccio alla sicurezza oppure sono stati ampliati con personale addetto alla sicurezza integrato o associato. Di conseguenza, i team prendono decisioni migliori sulla sicurezza nelle fasi iniziali del ciclo di sviluppo.

Anti-pattern comuni:

- Assegnazione di tutte le decisioni in materia di sicurezza al team responsabile della sicurezza.
- Gestione dei requisiti di sicurezza in fasi tardive del processo di sviluppo.
- Assenza di feedback di sviluppatori e responsabili della sicurezza sul funzionamento del programma.

Vantaggi dell'adozione di questa best practice:

- Riduzione del tempo necessario per completare le revisioni della sicurezza.
- Riduzione dei problemi di sicurezza rilevati solo in fase di revisione della sicurezza.
- Miglioramento della qualità complessiva del software compilato.
- Opportunità di identificare e comprendere i problemi sistematici o le aree di miglioramento a valore elevato.
- Riduzione della quantità di attività di correzione dovute agli esiti delle revisioni della sicurezza.
- Migliore percezione della funzione della sicurezza.

Livello di rischio associato se questa best practice non fosse adottata: basso

Guida all'implementazione

Per iniziare, attieniti alle linee guida illustrate in SEC11-BP01 Formazione per la sicurezza delle applicazioni Identifica quindi il modello operativo per il programma che ritieni più efficace per l'organizzazione. I due modelli principali consistono nel formare gli sviluppatori o nell'integrare responsabili della sicurezza nei team di sviluppo. Una volta scelto l'approccio iniziale, devi eseguire un progetto pilota con un singolo team o un piccolo gruppo di team del carico di lavoro per dimostrare il funzionamento del modello per l'organizzazione. Il supporto autorevole da parte dello sviluppatore e di altre parti responsabili della sicurezza dell'organizzazione semplifica l'implementazione e il successo del programma. Durante la creazione del programma, è importante scegliere le metriche da usare per dimostrarne il valore. Per un'ottima esperienza formativa, puoi documentarti sul modo in cui AWS ha affrontato questo problema. Questa best practice è per lo più incentrata sulla trasformazione e sulla cultura aziendali. Gli strumenti usati devono supportare la collaborazione tra lo sviluppatore e le comunità responsabili della sicurezza.

Passaggi dell'implementazione

- Per iniziare, predisponi corsi di formazione sulla sicurezza delle applicazioni per gli sviluppatori.
- Crea una community e un programma di onboarding per formare gli sviluppatori.
- Scegli un nome per il programma. Alcuni termini comunemente usati sono Responsabilità, Supporto o Promozione.
- Identifica il modello da usare: formazione per gli sviluppatori, integrazione di tecnici della sicurezza o ruoli di sicurezza per affinità.
- Identifica alcuni sponsor del progetto tra responsabili della sicurezza, sviluppatori e altri gruppi potenzialmente pertinenti.
- Tieni traccia delle metriche per il numero di persone coinvolte nel programma, del tempo impiegato per le revisioni e del feedback ottenuto da sviluppatori e responsabili della sicurezza. Usa queste metriche per apportare miglioramenti.

Risorse

Best practice correlate:

- SEC11-BP01 Formazione per la sicurezza delle applicazioni
- SEC11-BP02 Automazione dei test lungo il ciclo di vita di sviluppo e test

Documenti correlati:

- How to approach threat modeling
- How to think about cloud security governance
- How AWS built the Security Guardians program, a mechanism to distribute security ownership
- How to build a Security Guardians program to distribute security ownership

Video correlati:

- Proactive security: Considerations and approaches
- AppSec tooling and culture tips from AWS and Toyota Motor North America

Conclusioni

La sicurezza è una sfida costante. Quando si verificano, gli incidenti devono essere trattati come opportunità per migliorare la sicurezza dell'architettura. I controlli di identità avanzati, le risposte automatizzate agli eventi di sicurezza, l'infrastruttura protetta a più livelli e la gestione dei dati ben classificati tramite la crittografia forniscono una difesa avanzata che ogni organizzazione deve implementare. Questa operazione è semplificata grazie alle funzioni, alle AWS caratteristiche e ai servizi programmatici discussi in questo paper.

AWS si impegna ad aiutarvi a creare e gestire architetture che proteggono informazioni, sistemi e asset, offrendo al contempo valore aziendale.

Collaboratori

Le seguenti persone e organizzazioni hanno contribuito a questo documento:

- Jay Michael, Principal Security Lead Solutions Architect, Amazon Web Services
- Kiaan Sumeet, Principal Security Consultant, Amazon Web Services
- Michael Fischer, Principal Solutions Architect, Amazon Web Services
- Conor Colgan, Principal Solutions Architect, Amazon Web Services
- Dave Walker, Principal Solutions Architect, Security & Compliance, Amazon Web Services
- Patrick Palmer, Principal Solutions Architect, Security & Compliance, Amazon Web Services
- Monka Vu Minh, Security Consultant, Amazon Web Services
- Kurt Kumar, Security Consultant, Amazon Web Services
- Fahima Khan, Security Solutions Architect, Amazon Web Services
- Mutaz Hajeer, Senior Security Solutions Architect, Amazon Web Services
- Luis Pastor, Senior Security Solutions Architect, Amazon Web Services
- Colin Igbokwe, Senior Security Solutions Architect, Amazon Web Services
- Geoff Sweet, Senior Security Solutions Architect, Amazon Web Services
- Anthony Harvey, Senior Security Solutions Architect, Amazon Web Services
- Sowjanya Rajavaram, Senior Security Solutions Architect, Amazon Web Services
- Krishna Prasad, Senior Solutions Architect, Amazon Web Services
- Faisal Farooq, Senior Solutions Architect, Amazon Web Services
- Arun Krishnaswamy, Senior Solutions Architect, Amazon Web Services
- Dan Girard, Senior Solutions Architect, Amazon Web Services
- Marc Luescher, Senior Solutions Architect, Amazon Web Services
- Kyle Nicodemus, Senior Technical Account Manager, Amazon Web Services
- Irina Szabo, Senior Technical Account Manager, Amazon Web Services
- Arun Sivaraman, Solutions Architect, Amazon Web Services
- Stephen Novak, Technical Account Manager, Amazon Web Services
- Jonathan Risbrook, Technical Account Manager, Amazon Web Services
- Freddy Kasprzykowski, Practice Manager - Global Financial Services, Amazon Web Services
- Pat Gaw, Principal Security Consultant, Amazon Web Services

- Jason Garman, Principal Security Solutions Architect, Amazon Web Services
- Mark Keating, Principal Security Solutions Architect, Amazon Web Services
- Zach Miller, Principal Security Solutions Architect, Amazon Web Services
- Maitreya Ranganath, Principal Security Solutions Architect, Amazon Web Services
- Reef Dsouza, Principal Solutions Architect, Amazon Web Services
- Brad Burnett, Security Solutions Architect, Amazon Web Services
- Matt Saner, Senior Manager, Security Solutions Architecture, Amazon Web Services
- Priyank Ghedia, Senior Security Solutions Architect, Amazon Web Services
- Arthur Mnev, Senior Security Solutions Architect, Amazon Web Services
- Kyle Dickinson, Senior Security Solutions Architect, Amazon Web Services
- Kevin Boland, Senior Security Solutions Architect, Amazon Web Services
- Anna McAbee, Senior Security Solutions Architect, Amazon Web Services
- Recep Meric Degirmenci, Senior Security Solutions Architect, Amazon Web Services
- Daniel Salzedo, Senior Security Technical Product Manager, Amazon Web Services
- Jake Izumi, Senior Solutions Architect, Amazon Web Services
- Bert Bullough, Senior Solutions Architect, Amazon Web Services
- Robert McCall, Solutions Architect, Amazon Web Services
- Angela Chao, ESL TAM, AWS Enterprise Support, Amazon Web Services
- Pratima Singh, Senior ANZ Security Spec. Solutions Architect, Amazon Web Services
- Darran Boyd, Principal, Office of the CISO, AWS Security, Amazon Web Services
- Byron Pogson, Senior Security Solutions Architect, Amazon Web Services

Approfondimenti

Per ulteriore assistenza, consulta le seguenti risorse:

- Whitepaper sul Framework AWS Well-Architected
- AWS Architecture Center

Revisioni del documento

Per ricevere una notifica sugli aggiornamenti del presente whitepaper, iscriviti al feed RSS.

Modifica	Descrizione	Data
Linee guida sulle best practice aggiornate	Le best practice sono state aggiornate con nuove linee guida nelle seguenti aree: SEC 2, SEC 3, SEC 4, SEC 6, SEC 7, SEC 8, SEC 9, SEC 10 e SEC 11. Le linee guida sono state aggiornate e perfezionate in tutte le sezioni relative a questo pilastro.	6 novembre 2024
Linee guida sulle best practice aggiornate	Apportati aggiornamenti in tutto il pilastro su larga scala in merito alle best practice. Riordino e consolidamento di diverse best practice. Modifiche significative nelle SEC 1, 4, 5, 6, 7, 8 e 9.	27 giugno 2024
Linee guida sulle best practice aggiornate	Best practice aggiornate con nuove linee guida nelle seguenti aree: Gestione sicura dei carichi di lavoro e Protezione dei dati in transito.	6 dicembre 2023
Linee guida sulle best practice aggiornate	Principali aggiornamenti alle linee guida e alle best practice in Risposta agli incidenti. Diverse best practice aggiornate in Preparazione. Aggiunte due nuove aree	3 ottobre 2023

	alla risposta agli incidenti: Operazioni e Attività post-incidente. Aggiunta di nuove best practice a SEC10-BP08 Definizione di un framework per apprendere dagli incidenti.	
Linee guida sulle best practice aggiornate	Le best practice sono state aggiornate con nuove linee guida nelle seguenti aree: preparazione e simulazione.	13 luglio 2023
Aggiornamenti per il nuovo framework.	Best practice aggiornate con prontuario e nuove best practice aggiunte. È stata aggiunta una nuova area di best practice per Application Security (AppSec).	10 aprile 2023
Aggiornamento del whitepaper	Best practice aggiornate con nuova guida all'imple mentazione.	15 dicembre 2022
Aggiornamento del whitepaper	Ampliamento delle best practice e aggiunta dei piani di miglioramento.	20 ottobre 2022
Aggiornamento secondario	Informazioni IAM aggiornat e per allineamento alle best practice attuali.	28 giugno 2022
Aggiornamento secondario	Informazioni aggiuntive su AWS PrivateLink e correzione dei link danneggiati.	19 maggio 2022
Aggiornamento secondario	Aggiunto AWS PrivateLink.	6 maggio 2022
Aggiornamento secondario	Rimozione del linguaggio non inclusivo.	22 aprile 2022

Aggiornamento secondario	Aggiunte informazioni sullo strumento di analisi degli accessi alla rete VPC.	2 febbraio 2022
Aggiornamento secondario	Correzione di un link danneggiato.	27 maggio 2021
Aggiornamento secondario	Modifiche editoriali in varie parti del documento.	17 maggio 2021
Aggiornamento principale	Aggiunta una sezione sulla governance, aggiunti dettagli in varie sezioni, aggiunte nuove funzionalità e servizi in tutto il documento.	7 maggio 2021
Aggiornamento secondario	Link aggiornati.	10 marzo 2021
Aggiornamento secondario	Correzione di un link danneggiato.	15 luglio 2020
Aggiornamenti per il nuovo framework	Linee guida aggiornate sulla gestione di account, identità e autorizzazioni.	8 luglio 2020
Aggiornamenti per il nuovo framework	Aggiornamento per ampliare i consigli in ogni area, nuove best practice, servizi e funzionalità.	30 aprile 2020
Aggiornamento del whitepaper	Aggiornamenti che rispecchi ano i nuovi servizi e le nuove funzionalità di AWS; riferimenti aggiornati.	1° luglio 2018

Aggiornamento del whitepaper	La sezione aggiornata su configurazione e mantenimento della sicurezza del sistema presenta i nuovi servizi e le nuove funzionalità di AWS.	1 maggio 2017
Pubblicazione iniziale	Pubblicazione del pilastro della sicurezza: Framework AWS Well-Architected.	1° novembre 2016

Note

I clienti sono responsabili della propria valutazione indipendente delle informazioni contenute nel presente documento. Questo documento: (a) è solo a scopo informativo, (b) rappresenta le offerte e le pratiche attuali di AWS prodotti, che sono soggette a modifiche senza preavviso, e (c) non crea alcun impegno o assicurazione da parte dei suoi affiliati, AWS fornitori o licenzianti. AWS i prodotti o i servizi sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite. Le responsabilità e le responsabilità dei AWS propri clienti sono regolate da AWS accordi e il presente documento non fa parte di, né modifica, alcun accordo tra AWS e i suoi clienti.

AWS Glossario

Per la AWS terminologia più recente, consultate il AWS glossario nella sezione Reference.Glossario AWS