

Framework AWS Well-Architected

Pilastro della sicurezza



Pilastro della sicurezza: Framework AWS Well-Architected

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Riassunto e introduzione	1
Introduzione	1
Nozioni di base sulla sicurezza	3
Principi di progettazione	3
Definizione	4
Responsabilità condivisa	4
Governance	6
Gestione e separazione degli account AWS	8
SEC01-BP01 Separazione dei carichi di lavoro tramite account	9
SEC01-BP02 Utente root e proprietà dell'account sicuro	13
Gestione sicura dei carichi di lavoro	18
SEC01-BP03 Identificazione e convalida degli obiettivi di controllo	20
SEC01-BP04 Aggiornamento costante sulle minacce alla sicurezza	21
SEC01-BP05 Aggiornamento costante sulle raccomandazioni di sicurezza	21
SEC01-BP06 Automatizzazione dei test e della convalida dei controlli di sicurezza nelle pipeline	22
SEC01-BP07 Identificare le minacce e dare priorità alle mitigazioni utilizzando un modello di minaccia.	24
SEC01-BP08 Valutazione e implementazione periodiche di nuovi servizi e funzionalità di sicurezza	28
Gestione di identità e accessi	30
Gestione delle identità	30
SEC02-BP01 Utilizzo di meccanismi di accesso efficaci	31
SEC02-BP02 Utilizzo di credenziali temporanee	34
SEC02-BP03 Archiviazione e utilizzo dei segreti in modo sicuro	37
SEC02-BP04 Fai affidamento su un provider di identità centralizzato	43
SEC02-BP05 Verifica e rotazione periodica delle credenziali	47
SEC02-BP06 Utilizzo dei gruppi di utenti e degli attributi	50
Gestione delle autorizzazioni	51
SEC03-BP01 Definizione dei requisiti di accesso	54
SEC03-BP02 Concessione dell'accesso con privilegio minimo	56
SEC03-BP03 Determinazione di un processo per l'accesso di emergenza	60
SEC03-BP04 Riduzione delle autorizzazioni in modo continuo	68
SEC03-BP05 Definizione dei guardrail per le autorizzazioni dell'organizzazione	70

SEC03-BP06 Gestione degli accessi in base al ciclo di vita	72
SEC03-BP07 Analisi dell'accesso pubblico e multi-account	73
SEC03-BP08 Condivisione delle risorse in modo sicuro all'interno dell'organizzazione	75
SEC03-BP09 Condivisione sicura delle risorse con terze parti	80
Rilevamento	86
SEC04-BP01 Configurazione dei registri di servizi e applicazioni	87
Guida all'implementazione	10
Risorse	12
SEC04-BP02 Analisi di log, risultati e parametri a livello centrale	92
Guida all'implementazione	10
Risorse	12
SEC04-BP03 Automazione delle risposte agli eventi	94
Guida all'implementazione	10
Risorse	12
SEC04-BP04 Implementazione di eventi di sicurezza fruibili	96
Guida all'implementazione	10
Risorse	12
Protezione dell'infrastruttura	97
Protezione delle reti	98
SEC05-BP01 Creazione di livelli di rete	99
SEC05-BP02 Controllo del traffico a tutti i livelli	102
SEC05-BP03 Automatizzazione della protezione di rete	104
SEC05-BP04 Implementazione di funzioni di ispezione e protezione	106
Protezione delle risorse di calcolo	107
SEC06-BP01 Gestione delle vulnerabilità	108
SEC06-BP02 Riduzione della superficie d'attacco	111
SEC06-BP03 Implementazione di servizi gestiti	113
SEC06-BP04 Automatizzazione della protezione delle risorse di calcolo	114
SEC06-BP05 Concessione del permesso di eseguire azioni a distanza	116
SEC06-BP06 Convalida dell'integrità del software	117
Protezione dei dati	119
Classificazione dei dati	119
SEC07-BP01 Identificazione dei dati all'interno del carico di lavoro	119
SEC07-BP02 Definizione dei controlli di protezione dei dati	125
SEC07-BP03 Automazione dell'identificazione e della classificazione	126
SEC07-BP04 Definizione della gestione del ciclo di vita dei dati	127

Protezione dei dati inattivi	128
SEC08-BP01 Implementazione della gestione sicura delle chiavi	129
SEC08-BP02 Applicazione della crittografia dei dati inattivi	133
SEC08-BP03 Automatizzazione della protezione dei dati a riposo	135
SEC08-BP04 Applicazione del controllo degli accessi	136
SEC08-BP05 Utilizzo di meccanismi per tenere le persone a distanza dai dati	139
Protezione dei dati in transito	140
SEC09-BP01 Implementazione della gestione sicura delle chiavi e dei certificati	141
SEC09-BP02 Applicazione della crittografia dei dati in transito	144
SEC09-BP03 Automatizzazione del rilevamento degli accessi indesiderati ai dati	147
SEC09-BP04 Autenticazione delle comunicazioni di rete	147
Risposta agli imprevisti	153
Risposta agli incidenti di AWS	153
Progettazione degli obiettivi di risposta al cloud	154
Preparazione	155
SEC10-BP01 Identificazione del personale chiave e delle risorse esterne	156
SEC10-BP02 Sviluppo di piani di gestione degli incidenti	157
SEC10-BP03 Preparazione di funzionalità forensi	161
SEC10-BP04 Sviluppo e test di playbook di risposta agli incidenti di sicurezza	164
SEC10-BP05 Preassegnazione dell'accesso	166
SEC10-BP06 Distribuzione anticipata degli strumenti	170
SEC10-BP07 Esecuzione di simulazioni	173
Operazioni	175
Attività post-incidente	176
SEC10-BP08 Definizione di un framework per apprendere dagli incidenti	177
Sicurezza delle applicazioni	180
SEC11-BP01 Formazione per la sicurezza delle applicazioni	181
Guida all'implementazione	10
Risorse	12
SEC11-BP02 Automazione dei test lungo il ciclo di vita di sviluppo e test	184
.....	184
.....	184
Guida all'implementazione	10
Risorse	12
SEC11-BP03 Esecuzione di test di penetrazione (pen-test) a intervalli regolari	187
Guida all'implementazione	10

Risorse	12
SEC11-BP04 Revisioni manuali del codice	190
Guida all'implementazione	10
Risorse	191
SEC11-BP05 Centralizzazione dei servizi per pacchetti e dipendenze	192
Guida all'implementazione	10
Risorse	12
SEC11-BP06 Implementazione programmatica del software	194
Guida all'implementazione	10
Risorse	12
SEC11-BP07 Valutazione regolare delle proprietà di sicurezza delle pipeline	196
Guida all'implementazione	10
Risorse	12
SEC11-BP08 Creazione di un programma per l'integrazione della titolarità della sicurezza nei team responsabili del carico di lavoro	198
Guida all'implementazione	10
Risorse	12
Conclusione	201
Collaboratori	202
Approfondimenti	203
Revisioni del documento	204
Avvisi	207

Pilastro della sicurezza - Framework AWS Well-Architected

Data di pubblicazione: 6 dicembre 2023 ([Revisioni del documento](#))

Questo whitepaper tratta del principio della sicurezza del [Framework AWS Well-Architected](#). Fornisce istruzioni per aiutarti ad applicare le best practice e le raccomandazioni correnti nella progettazione, distribuzione e manutenzione di carichi di lavoro sicuri in AWS.

Introduzione

Al [Framework AWS Well-Architected](#) aiuta a comprendere i pro e i contro delle decisioni che vengono prese durante la progettazione dei 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. Permette 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 architettati aumenta notevolmente la probabilità di successo aziendale.

Il Canone si basa su sei principi:

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

Questo whitepaper tratta del principio 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 asset in modo da migliorare la sicurezza. Questo 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:

- **Implementa una solida base di identità:** implementa il principio del privilegio minore e attua la separazione dei compiti con la corretta autorizzazione per ciascuna interazione con le risorse AWS. Centralizza la gestione delle identità e mira a eliminare la dipendenza dalle credenziali statiche a lungo termine.
- **Mantieni la tracciabilità:** monitora, avvisa e verifica le azioni e le modifiche al tuo ambiente in tempo reale. Integra la raccolta di log e parametri con i sistemi per analizzare e intervenire automaticamente.
- **Applica la 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).
- **Automatizza le best practice per la sicurezza:** I meccanismi di sicurezza automatici basati sul software migliorano la tua capacità di ridimensionare in modo sicuro, più rapido e conveniente. Crea architetture sicure, compresa l'implementazione dei controlli, che sono definite e gestite come codice nei modelli controllati dalle versioni.
- **Proteggi i dati in transito e a riposo:** classifica i dati secondo livelli di sensibilità e meccanismi d'uso, come crittografia, tokenizzazione e controllo di accesso, ove opportuno.
- **Tieni le persone a distanza dai 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.
- **Preparati per gli eventi di sicurezza:** Preparati per un incidente ipotetico creando policy e processi di gestione degli incidenti allineati ai 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 di identità e accessi](#)
- [Rilevamento](#)
- [Protezione dell'infrastruttura](#)
- [Protezione dei dati](#)
- [Risposta agli imprevisti](#)
- [Sicurezza delle applicazioni](#)

Responsabilità condivisa

La sicurezza e la conformità sono una responsabilità condivisa da 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 ai servizi utilizzati, all'integrazione di tali servizi nel loro ambiente IT e alle leggi e ai regolamenti applicabili. La natura di questa responsabilità condivisa fornisce inoltre la flessibilità e il controllo dei clienti che consentono la distribuzione. Come mostrato nel grafico seguente, la distinzione della responsabilità è comunemente riferita alla sicurezza "del" cloud rispetto alla sicurezza "nel" cloud.

Responsabilità di AWS "Sicurezza del cloud" - AWS è responsabile della protezione dell'infrastruttura su cui vengono eseguiti tutti i servizi offerti nel Cloud AWS. Questa infrastruttura è composta da hardware, software, reti e strutture che eseguono i servizi Cloud AWS.

Responsabilità del cliente "Sicurezza nel cloud" - La responsabilità del cliente sarà determinata dai servizi del Cloud AWS selezionati dal cliente. 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 distribuiscono 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 ogni 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 appropriate.

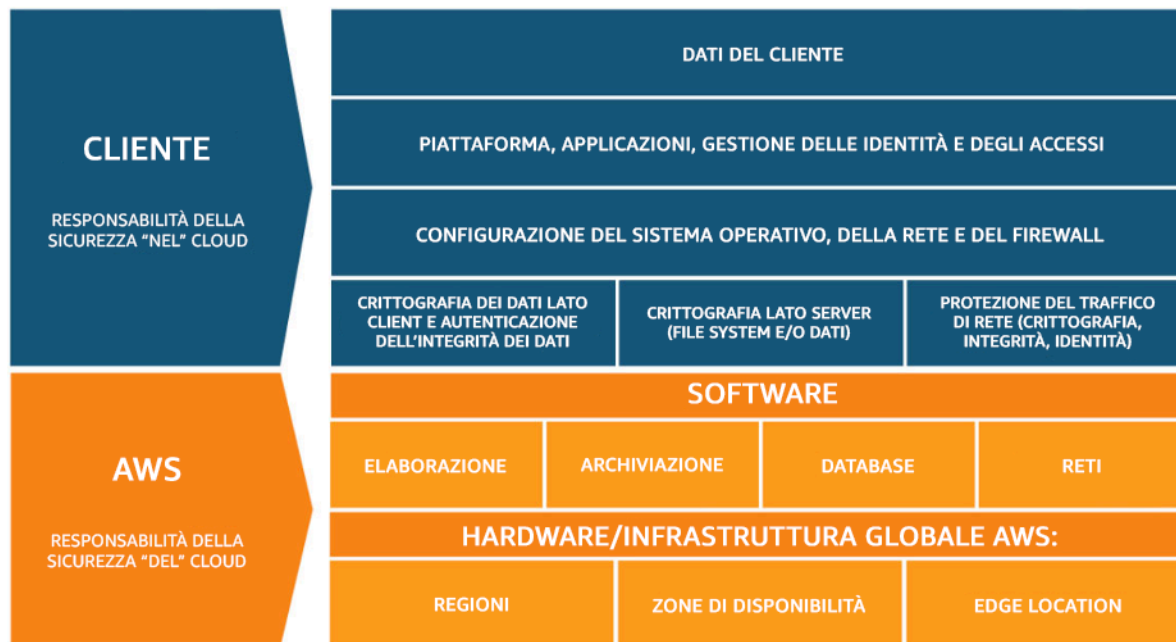


Figura 1: modello di responsabilità condivisa AWS.

Questo modello di responsabilità condivisa tra AWS/cliente si estende anche ai controlli IT. Così come la responsabilità di operare l'ambiente IT viene condivisa tra AWS e i suoi clienti, allo stesso modo vengono condivisi la gestione, l'operatività e la verifica dei controlli IT. AWS può aiutare a sollevare il cliente dal peso di gestire i controlli, occupandosi di tali controlli associati all'infrastruttura fisica distribuita nell'ambiente AWS che in precedenza poteva essere stato gestito dal cliente. Poiché ogni cliente in AWS ha una diversa distribuzione, i clienti 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. Alcuni 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 dei sistemi operativi, dei database e delle 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 che distribuiscono all'interno dei servizi AWS. Alcuni 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, ha il compito di supportare gli obiettivi aziendali definendo policy e controllando l'operato per contribuire alla gestione del rischio. Ottieni 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 modelli 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 è [AWS Artifact](#), che consente l'accesso on demand ai report di sicurezza e conformità di AWS e seleziona gli 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 provider di identità come AWS IAM Identity

Center e i controlli di rilevamento comuni. Qui si trovano anche alcuni degli output del processo di governance della piattaforma. Quando 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 in cui viene eseguita l'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 perché l'implementazione viene eseguita nelle applicazioni controllate dai team di prodotto. Potrebbe trattarsi dell'implementazione della convalida degli input in un'applicazione o della verifica che l'identità passi correttamente 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: evidenziare il rischio in base alle probabilità e alle conseguenze. Questo è il rischio inerente. 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 residuale. 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.

Probabilità	Livello di rischio				
Molto probabile	Bassa	Media	Alta	Critica	Critica
Probabile	Bassa	Media	Media	Alta	Critica
Possibile	Bassa	Bassa	Media	Media	Alta
Improbabile	Bassa	Bassa	Media	Media	Alta
Molto improbabile	Bassa	Bassa	Bassa	Media	Alta
Conseguenza	Minima	Bassa	Media	Alta	Severa

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 alla funzione, ai requisiti di conformità o a un set comune di controlli anziché riflettere la struttura della reportistica dell'organizzazione. In AWS, gli account rappresentano un confine difficile. 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.

Gestisci gli account centralmente: AWS Organizations [automatizza la creazione e la gestione di account AWS](#) e il controllo di tali account 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.

Imposta i controlli centralmente: 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 utenti e ruoli [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, automatizza il provisioning, applica [guardrail](#) (che includono prevenzione e rilevamento) e fornisce un pannello di controllo per la visibilità.

Configura servizi e risorse centralmente: AWS Organizations ti aiuta a configurare [servizi AWS](#) applicabili a tutti gli account. Ad esempio, puoi configurare la registrazione centralizzata di tutte le operazioni eseguite nell'organizzazione utilizzando [AWS CloudTrail](#) impedire agli account dei membri di disattivare l'attività di log. Puoi inoltre aggregare centralmente i dati per le regole definite utilizzando [AWS Config](#), il che ti consente di controllare i 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 attraverso una strategia multi-account. La separazione a livello di account è fortemente consigliata, in quanto fornisce un solido margine di isolamento per la sicurezza, la fatturazione e l'accesso.

Risultato desiderato: una struttura di account che isola le operazioni cloud, i carichi di lavoro non correlati e gli ambienti in account separati, aumentando la sicurezza dell'infrastruttura cloud.

Anti-pattern comuni:

- Inserimento di più carichi di lavoro non correlati con diversi livelli di sensibilità dei dati nello stesso account.
- Struttura dell'unità organizzativa (UO) scarsamente definita.

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 con policy e amministrazione centralizzata dei servizi di sicurezza.
- Processo automatizzato di creazione e mantenimento dell'account.
- Audit centralizzato 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 avere una guida su concetti, modelli e implementazione di una strategia multi-account su AWS, consulta [Organizing Your AWS Environment Using Multiple Accounts](#) (Organizzazione dell'ambiente AWS con l'utilizzo di account multipli).

Se si dispone di più Account AWS, gli account devono essere organizzati 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 membro 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 ottenere i controlli desiderati per ogni account membro.

[AWS Organizations](#) e [AWS Control Tower](#) sono due servizi che possono essere utilizzati 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, ognuna delle quali contiene una serie di account membri. Le [policy di controllo dei servizi](#) consentono

all'amministratore dell'organizzazione di stabilire controlli preventivi granulari sugli account dei membri, mentre [AWS Config](#) può essere utilizzato per stabilire controlli proattivi e investigativi sugli account dei membri. Molti servizi AWS [si integrano con AWS Organizations](#) per fornire controlli amministrativi delegati e per eseguire attività specifiche del servizio su tutti gli account dei membri dell'organizzazione.

Posizionato sopra AWS Organizations, [AWS Control Tower](#) fornisce un'impostazione delle best practice in un solo clic 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:

- Guardrail di sicurezza obbligatori integrati che vengono applicati automaticamente agli account ammessi nell'organizzazione.
- Guardrail opzionali che possono essere attivati o disattivati per un determinato insieme di unità organizzative.
- [AWS Control Tower Account Factory](#) fornisce l'implementazione automatica di account contenenti linee di base e opzioni di configurazione pre-approvate all'interno dell'organizzazione.

Passaggi dell'implementazione

1. Progettazione di una struttura organizzativa unitaria: una struttura di unità organizzative opportunamente studiata riduce l'onere di gestione necessario per creare e mantenere le policy di controllo dei servizi e gli altri controlli di sicurezza. La struttura delle unità organizzative deve essere [allineata alle esigenze aziendali, alla sensibilità dei dati e alla struttura del carico di lavoro](#).
2. Creazione di una zona di destinazione per l'ambiente multi-account: una zona di destinazione fornisce una base di sicurezza e infrastruttura coerente da cui l'organizzazione può sviluppare, lanciare e implementare rapidamente i carichi di lavoro. Puoi utilizzare una [zona di destinazione personalizzata o AWS Control Tower](#) per orchestrare il tuo ambiente.
3. Realizzazione di guardrail: implementa guardrail di sicurezza coerenti per il tuo ambiente attraverso la zona di destinazione. AWS Control Tower offre un elenco di controlli implementabili [obbligatori](#) e [facoltativi](#). I controlli obbligatori vengono implementati automaticamente quando si utilizza Control Tower. Esamina l'elenco dei controlli altamente consigliati e facoltativi e adotta quelli più adatti alle tue esigenze.
4. Accesso limitato a Regioni aggiunte di recente: per le nuove Regioni AWS, le risorse IAM, ad esempio utenti e ruoli, verranno propagate solo alle Regioni specificate. Questa azione può

essere eseguita tramite la [console quando si utilizza Control Tower](#) oppure regolando le [policy di autorizzazione IAM in AWS Organizations](#).

5. Presa in esame di AWS [CloudFormation StackSets](#): StackSets consente di implementare risorse, tra cui policy, ruoli e gruppi IAM in Account AWS e Regioni differenti a partire da un modello approvato.

Risorse

Best practice correlate:

- [SEC02-BP04 Fai affidamento su un provider di identità centralizzato](#)

Documenti correlati:

- [AWS Control Tower](#)
- [Linee guida sugli audit di sicurezza AWS](#)
- [IAM Best Practices](#)(Best Practice IAM)
- [Use CloudFormation StackSets to provision resources across multiple Account AWS and regions](#) (Utilizzo di StackSet CloudFormation per il provisioning delle risorse su più account e regioni AWS)
- [Organizations FAQ](#) (Domande frequenti sulle organizzazioni)
- [AWS Organizations Concetti e terminologia](#)
- [Best Practices for Service Control Policies in an AWS Organizations Multi-Account Environment](#) (Best practice per le policy di controllo dei servizi di AWS Organizations in un ambiente multi-account)
- [Guida di riferimento per la gestione degli account AWS](#)
- [Organizzazione dell'ambiente AWS con l'utilizzo di account multipli](#)

Video correlati:

- [Enable AWS adoption at scale with automation and governance](#) (Consentire l'adozione di AWS su larga scala con l'automazione e la governance)
- [Security Best Practices the Well-Architected Way](#)
- [Building and Governing Multiple Accounts using AWS Control Tower](#) (Creazione e gestione di account multipli con AWS Control Tower)

- [Enable Control Tower for Existing Organizations](#) (Abilitare la Control Tower per le organizzazioni esistenti)

Workshop correlati:

- [Control Tower Immersion Day](#) (Giornata di approfondimento su Control Tower)

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. Disabilitare 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: la sicurezza dell'utente root contribuisce a ridurre la possibilità che si verifichino danni accidentali o intenzionali a causa dell'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 delle infrastrutture critiche, dei processi e del 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 derivanti dall'adozione di questa best practice: proteggere l'accesso all'utente root crea la certezza che le azioni del proprio account siano controllate e sottoposte a audit.

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 abilitate per impostazione predefinita, è necessario intervenire direttamente per implementarle. Queste raccomandazioni sono 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.

Quando si crea un Account AWS per la prima volta, si inizia 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. È possibile accedere come utente root mediante l'indirizzo e-mail e la password usati per creare l'account. A causa dei livelli elevati di accesso concessi all'utente root AWS, è necessario limitare l'uso dell'utente root AWS all'esecuzione di attività che [lo richiedono specificamente](#). Le credenziali di accesso dell'utente root devono essere tenute sotto stretta sorveglianza e l'autenticazione a più fattori (MFA) deve essere sempre abilitata 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. Considerare anche 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, ognuno dei quali ha un utente root. Un account è designato come account di gestione e sotto l'account di gestione possono essere aggiunti 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 le seguenti fasi di implementazione. Eventuali raccomandazioni sono collegate a [CIS AWS Foundations benchmark versione 1.4.0](#). Oltre a questi passaggi, consulta le [AWS best practice guidelines](#) (Linee guida sulle best practice AWS) per la protezione delle risorse e degli Account AWS.

Controlli preventivi

1. Imposta [informazioni di contatto](#) accurate 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 piuttosto che dell'account di 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 per l'utente root, è necessario passare i processi che utilizzano tali chiavi all'uso di chiavi di accesso temporanee di un ruolo AWS Identity and Access Management (IAM), quindi [eliminare le chiavi di accesso per l'utente root](#).
3. Stabilisci se è necessario memorizzare le credenziali per l'utente root.
 - a. Se utilizzi AWS Organizations per creare nuovi account membro, la password iniziale dell'utente root sui nuovi account membro è impostata su un valore casuale che non è visibile a te. Considera l'utilizzo del flusso di ripristino della password dal tuo account di gestione di AWS Organization per [ottenere l'accesso 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. Abilita la MFA per l'utente root.
4. Abilita i controlli preventivi per gli utenti root degli account membri in ambienti multi-account AWS.
 - a. Considera di attivare il guardrail preventivo [Disallow Creation of Root Access Keys for the Root User](#) (Disabilitare la creazione di chiavi di accesso root per l'utente root) per gli account dei membri.
 - b. Considera di attivare il guardrail preventivo [Disallow Actions as a Root User](#) (Disabilitare le azioni come utente root) per gli account dei membri.
5. Se sono necessarie le credenziali per l'utente root:

- a. Utilizza una password complessa.
 - b. Abilita l'autenticazione a più fattori (MFA) per l'utente root, in particolare per gli account dei manager (paganti) AWS Organizations (CIS 1.5).
 - c. Considera 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 abilitare un [dispositivo MFA](#) o [virtuale o hardware](#).
 - d. Considera la possibilità di iscrivere più dispositivi MFA per il backup. [Sono consentiti fino a 8 dispositivi MFA per account](#).
 - Tieni presente che l'iscrizione di più di un dispositivo MFA per l'utente root disabilita automaticamente il [flusso per il recupero dell'account in caso di perdita 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 della password dell'utente root](#) su base periodica riduce il rischio che una password esposta inavvertitamente possa essere utilizzata in modo improprio.

Controlli di rilevamento

- Crea allarmi per rilevare l'uso delle credenziali root (CIS 1.7). [L'abilitazione di Amazon GuardDuty](#) monitorerà e segnalerà l'uso delle credenziali API dell'utente root attraverso il rilevamento [RootCredentialUsage](#).
- Valuta e implementa i controlli investigativi inclusi in [AWS Well-Architected Security Pillar conformance pack for AWS Config](#) (Pacchetto di conformità del pilastro di sicurezza well-architected di AWS per AWS Config) oppure, se si utilizza 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 dell'account AWS non deve essere utilizzato per le attività giornaliere e nemmeno per quelle amministrative. Effettua il login come utente root solo per eseguire [attività AWS che lo richiedono](#). 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 periodicamente che l'indirizzo e-mail associato all'account e quelli elencati in [Alternate Contacts](#) (Contatti alternativi) funzionino. 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](#) (Guida alla risposta agli incidenti di sicurezza AWS) e alle best practice riportate nella [sezione Incident Response \(Risposta agli incidenti\) del whitepaper Security Pillar \(Pilastro di sicurezza\)](#) per ulteriori informazioni sulla creazione di una strategia di risposta agli incidenti del tuo Account AWS.

Risorse

Best practice correlate:

- [SEC01-BP01 Separazione dei carichi di lavoro tramite account](#)
- [SEC02-BP01 Utilizzo 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](#)
- [Linee guida sugli audit di sicurezza AWS](#)
- [IAM Best Practices](#)(Best Practice IAM)
- [Amazon GuardDuty – root credential usage alert](#) (Amazon GuardDuty – Avviso sull'utilizzo delle credenziali root)
- [Step-by-step guidance on monitoring for root credential use through CloudTrail](#) (Guida passo-passo sul monitoraggio dell'uso delle credenziali root tramite CloudTrail)
- [Token MFA approvati per l'uso con AWS](#)
- Implementazione di funzionalità di [break glass access](#) (accesso di emergenza) su AWS
- [Top 10 security items to improve in your Account AWS](#) (I 10 principali elementi di sicurezza da migliorare nel proprio account AWS)
- [Che cosa devo fare se noto un'attività non autorizzata nel mio Account AWS?](#)

Video correlati:

- [Enable AWS adoption at scale with automation and governance](#) (Consentire l'adozione di AWS su larga scala con l'automazione e la governance)
- [Security Best Practices the Well-Architected Way](#)
- [Limiting use of AWS root credentials](#) (Restrizioni nell'uso delle credenziali AWS) da AWS re:inforce 2022 – Security best practices with AWS IAM (Best practice di sicurezza con AWS IAM)

Esempi e laboratori correlati:

- [Laboratorio: Account AWS e utente root](#)

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 alle continue migliorie. Uno dei modi per migliorare la tua capacità di agire in sicurezza nel cloud è avere 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 sono appropriati per quel carico di lavoro?". Avere un approccio coerente alle decisioni velocizza la distribuzione 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 ricalibrare 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 cosa in maniera ripetuta senza errori non è possibile. Anche con runbook scritti correttamente, corri il rischio che le persone non eseguano correttamente 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 distribuire le applicazioni è attraverso l'automazione. Il codice che esegue la distribuzione può essere testato e poi utilizzato per eseguire la distribuzione stessa. Questo aumenta la sicurezza nel processo di cambiamento 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 distribuita 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 distribuzione, riducendo così un'eventuale rielaborazione. Per ridurre la possibilità di errori di distribuzione, effettua le modifiche di configurazione tramite codice e non tramite le persone. Se hai bisogno di distribuire nuovamente un'applicazione, l'automazione rende questa operazione molto più semplice. 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 registrazione comune 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 costante sulle minacce alla sicurezza](#)
- [SEC01-BP05 Aggiornamento costante sulle raccomandazioni di sicurezza](#)
- [SEC01-BP06 Automatizzazione dei test e della convalida dei controlli di sicurezza nelle pipeline](#)
- [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, deriva 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.

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

Guida all'implementazione

- Identifica i requisiti di conformità. Scopri i requisiti organizzativi, legali e di conformità perché il tuo carico di lavoro risulti conforme.
- Identifica le risorse di conformità AWS: identifica le risorse che AWS mette a disposizione per aiutarti nei processi di conformità.
 - <https://aws.amazon.com/compliance/>
 - <https://aws.amazon.com/artifact/>

Risorse

Documenti correlati:

- [AWS Security Audit Guidelines](#)
- [Bollettini sulla sicurezza](#)

Video correlati:

- [AWS Security Hub: gestire gli avvisi di sicurezza e automatizzare la conformità](#)
- [Security Best Practices the Well-Architected Way](#)

SEC01-BP04 Aggiornamento costante sulle minacce alla sicurezza

Per definire e implementare controlli appropriati, riconosci i vettori di attacco rimanendo aggiornato sulle minacce alla sicurezza più recenti. Usa AWS Managed Services per semplificare la ricezione di notifiche in seguito a comportamenti inaspettati o inusuali nei tuoi account AWS. Esegui delle indagini avvalendoti degli strumenti AWS Partner o di feed di informazioni sulle minacce di terze parti come parte del tuo flusso di informazioni di sicurezza. Al [CVE \(Common Vulnerabilities and Exposures\)](#) contiene vulnerabilità di sicurezza informatica pubbliche che puoi utilizzare come aggiornamento.

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

Guida all'implementazione

- Iscrizione alle fonti di informazione sulle minacce: consulta regolarmente le informazioni sulle minacce da varie fonti attinenti alle tecnologie che utilizzi per il tuo carico di lavoro.
 - [Elenco CVE \(Common Vulnerabilities and Exposures\)](#)
- Considera il servizio [AWS Shield Advanced](#) : fornisce visibilità quasi in tempo reale sulle fonti di intelligence, se il tuo carico di lavoro è accessibile da Internet.

Risorse

Documenti correlati:

- [AWS Security Audit Guidelines](#)
- [AWS Shield](#)
- [Bollettini sulla sicurezza](#)

Video correlati:

- [Security Best Practices the Well-Architected Way](#)

SEC01-BP05 Aggiornamento costante sulle raccomandazioni di sicurezza

Tieniti aggiornato sulle raccomandazioni di sicurezza di AWS e del settore, così da revisionare l'assetto di sicurezza del tuo carico di lavoro. [Bollettini sulla sicurezza AWS](#) contengono informazioni importanti sulla sicurezza e notifiche relative alla privacy.

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

Guida all'implementazione

- Segui gli aggiornamenti di AWS: segui o verifica regolarmente la presenza di nuovi consigli, suggerimenti e trucchi.
 - [AWS Well-Architected Labs](#)
 - [Blog sulla sicurezza AWS](#)
 - [Documentazione del servizio AWS](#)
- Sottoscrivi gli aggiornamenti di settore: consulta regolarmente le notizie da varie fonti attinenti alle tecnologie impiegate nel tuo carico di lavoro.
 - [Esempio: Elenco CVE \(Common Vulnerabilities and Exposures\)](#)

Risorse

Documenti correlati:

- [Bollettini sulla sicurezza](#)

Video correlati:

- [Security Best Practices the Well-Architected Way](#)

SEC01-BP06 Automatizzazione dei test e della convalida dei controlli di sicurezza nelle pipeline

Stabilisci previsioni e modelli sicuri per i meccanismi di sicurezza testati e convalidati come parte della compilazione, delle pipeline e dei processi. Utilizza strumenti e l'automazione per testare e convalidare tutti i controlli di sicurezza in modo continuo. Ad esempio, scansiona elementi quali immagini di macchine e modelli di infrastrutture come codice per individuare vulnerabilità di sicurezza, irregolarità e deviazioni da una previsione stabilita in ogni fase. AWS CloudFormation Guard può aiutarti a verificare la sicurezza dei modelli CloudFormation, a risparmiare tempo e a ridurre il rischio che si verifichino errori di configurazione.

È fondamentale ridurre il numero di errori di sicurezza introdotti in un ambiente di produzione, quindi più operazioni di controllo di qualità e riduzione dei difetti è possibile eseguire nel processo di

compilazione, più efficace sarà il risultato. Progetta pipeline di integrazione e distribuzione continue (CI/CD) per testare eventuali problemi di sicurezza quando possibile. Le pipeline CI/CD offrono l'opportunità di migliorare la sicurezza in ogni fase della compilazione e della distribuzione. Anche gli strumenti di sicurezza CI/CD devono essere mantenuti aggiornati per mitigare le minacce in continua evoluzione.

Monitora le modifiche alla configurazione del tuo carico di lavoro per facilitare gli audit di conformità, la gestione delle modifiche e le indagini che possono essere applicate al tuo caso. Puoi usare AWS Config per registrare e valutare le tue risorse AWS e di terze parti. Consente di eseguire audit costanti e di valutare la conformità generale a regole e pacchetti di conformità, ossia raccolte di regole con azioni di correzione.

Nel monitoraggio delle modifiche sono incluse modifiche pianificate, parte del processo di controllo delle modifiche della tua organizzazione (a cui a volte si fa riferimento con l'acronimo MACD: Move, Add, Change, Delete), le modifiche non pianificate e le modifiche inaspettate, come gli incidenti. Le modifiche possono avvenire a livello di infrastruttura, ma essere relative anche ad altre categorie, come le modifiche nei repository di codice, le modifiche delle immagini di macchine e degli inventari di applicazioni, le modifiche di processi e policy o le modifiche alla documentazione.

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

Guida all'implementazione

- Automazione della gestione della configurazione: applica e convalida in automatico configurazioni sicure sfruttando un apposito servizio o strumento di gestione.
 - [AWS Systems Manager](#)
 - [AWS CloudFormation](#)
 - [Configurazione di una pipeline CI/CD in AWS](#)

Risorse

Documenti correlati:

- [Come usare le policy di controllo dei servizi per impostare guardrail di permessi negli account della tua AWS Organization](#)

Video correlati:

- [Gestire ambienti AWS multi-account tramite AWS Organizations](#)
- [Security Best Practices the Well-Architected Way](#)

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. Rivedi 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 ha lo scopo di identificare, comunicare e comprendere le minacce e le mitigazioni nel contesto della protezione di qualcosa di valore." – [The Open Web Application Security Project \(OWASP\) Application Threat Modeling](#)

Perché realizzare un modello di minaccia?

I sistemi sono complessi e nel tempo diventano sempre più complessi 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 e per elaborare le mitigazioni e 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 fornire 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 del settore](#). 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 è necessario eseguire la modellazione delle minacce?

La modellazione delle minacce deve essere avviata il più presto 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 rivisti 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

Come possiamo 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 possibile è iniziare con [Shostack's 4 Question Frame for Threat Modeling](#), che pone domande aperte per strutturare l'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 il modo più diffuso per rispondere a questa domanda, in quanto aiuta a visualizzare ciò che si sta costruendo, ad esempio utilizzando un [diagramma di flusso dei dati](#). Scrivere le ipotesi e i 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 costruendo 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. Cosa può andare storto?

In questa fase si identificano le minacce al sistema. Le minacce sono azioni o eventi accidentali o intenzionali che hanno 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 di tutti i componenti del team e dei [soggetti coinvolti](#) nell'esercizio di modellazione delle minacce. Per facilitare il brainstorming si può utilizzare un modello per l'identificazione delle minacce, ad esempio [STRIDE](#), che suggerisce diverse categorie da valutare: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of privilege (spoofing, manomissione, ripudio, divulgazione di informazioni, negazione del servizio ed elevazione dei privilegi). Inoltre, per facilitare il brainstorming, si possono consultare gli elenchi e le ricerche esistenti per trarne ispirazione, come ad esempio [OWASP Top 10](#), [HiTrust Threat Catalog](#) e il catalogo delle minacce della propria organizzazione.

3. Che cosa faremo a questo proposito?

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.

La sicurezza e la conformità sono una [responsabilità condivisa da AWS e dal cliente](#). È importante capire che quando si chiede "Che cosa faremo?", 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.

Per la parte AWS relativa alla responsabilità condivisa, si scoprirà 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 sono disponibili per il download 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 registrazione e il monitoraggio. La documentazione di ogni servizio AWS ha un [capitolo sulla sicurezza dedicato](#) che fornisce indicazioni sui controlli di sicurezza da considerare come mitigazioni. È importante considerare il codice che si sta scrivendo e le sue dipendenze e pensare ai controlli che si possono mettere in atto per affrontare queste minacce. Questi controlli possono essere elementi come 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. Abbiamo fatto un buon lavoro?

L'obiettivo è che il team e l'organizzazione migliorino sia la qualità dei modelli di minacce sia la velocità con cui vengono eseguiti nel tempo. Questi miglioramenti derivano da una combinazione di pratica, apprendimento, insegnamento e revisione. Per approfondire e mettere mano alla situazione, è consigliabile completare il corso di formazione [Threat modeling the right way for builders](#) (Come modellare le minacce nel modo giusto per gli sviluppatori) o il [workshop](#) insieme al team. Inoltre, se si desidera una guida su come integrare la modellazione delle minacce nel ciclo di vita dello sviluppo dell'applicazione della propria organizzazione, invitiamo a consultare il post [How to approach threat modeling](#) (Come affrontare la modellazione delle minacce) su AWS Security Blog (Blog sulla sicurezza AWS).

Threat Composer

Come ausilio nella modellazione delle minacce, puoi utilizzare lo 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 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 riferimenti, visita la pagina relativa allo strumento Threat Composer e passa all'area di lavoro di esempio definita dal sistema.

Risorse

Best practice correlate:

- [SEC01-BP03 Identificazione e convalida degli obiettivi di controllo](#)
- [SEC01-BP04 Aggiornamento costante sulle minacce alla sicurezza](#)

- [SEC01-BP05 Aggiornamento costante sulle raccomandazioni di sicurezza](#)
- [SEC01-BP08 Valutazione e implementazione periodiche di nuovi servizi e funzionalità di sicurezza](#)

Documenti correlati:

- [How to approach threat modeling](#) (AWS Security Blog)
- [NIST: Guide to Data-Centric System Threat Modelling](#)

Video correlati:

- [AWS Summit ANZ 2021 – How to approach threat modelling](#) (Summit ANZ 2021 – Come affrontare la modellazione delle minacce)
- [AWS Summit ANZ 2022 - Scaling security – Optimise for fast and secure delivery](#) (Summit ANZ 2022 - Scalare la sicurezza - Ottimizzare la consegna rapida e sicura)

Training correlati:

- [Threat modeling the right way for builders – AWS Skill Builder virtual self-paced training](#) (La corretta modellazione delle minacce per gli sviluppatori – Formazione virtuale autogestita Skill Builder)
- [Threat modeling the right way for builders – AWS Workshop](#) (La corretta modellazione delle minacce per gli sviluppatori – 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. Il blog sulla sicurezza AWS evidenzia nuovi servizi e funzionalità AWS, guide all'implementazione e linee guida generali sulla sicurezza. [Novità di AWS](#) è un'ottima scelta per essere aggiornati su tutte le nuove funzionalità, i servizi e gli annunci AWS.

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

Guida all'implementazione

- Pianificazione di revisioni regolari: crea un calendario di attività di revisione che preveda requisiti di conformità, valutazione delle nuove funzionalità e dei nuovi servizi di sicurezza AWS e l'aggiornamento costante rispetto alle novità del settore.
- Funzionalità e servizi AWS: scopri le funzionalità di sicurezza disponibili per i servizi che utilizzi e approfondisci le nuove caratteristiche al momento del rilascio.
 - [Blog sulla sicurezza AWS](#)
 - [Bollettini sulla sicurezza AWS](#)
 - [Documentazione del servizio AWS](#)
- Definizione del processo di onboarding del servizio AWS: definisci i processi per l'onboarding di nuovi servizi AWS. Includi il modo in cui valuti la funzionalità dei nuovi servizi AWS e i requisiti di conformità per il tuo carico di lavoro.
- Test di nuovi servizi e funzionalità: testa nuovi servizi e funzionalità al momento del rilascio in un ambiente non di produzione che replica in maniera fedele quello di produzione.
- Implementazione di altri meccanismi di difesa: implementa meccanismi automatizzati per difendere il carico di lavoro, esplora le opzioni disponibili.
 - [Correzione di risorse AWS non conformi in base alle regole di Regole di AWS Config](#)

Risorse

Video correlati:

- [Security Best Practices the Well-Architected Way](#)

Gestione di identità e 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](#)
- [Gestione delle autorizzazioni](#)

Gestione delle identità

Ci sono due tipi di identità da gestire quando ci si avvicina all'utilizzo di carichi di lavoro AWS sicuri.

- **Identità umane:** gli amministratori, gli sviluppatori, gli operatori e i fruitori di applicazioni necessitano di un'identità per accedere agli ambienti e alle applicazioni AWS. Possono essere membri dell'organizzazione o utenti esterni con cui collabori e che interagiscono con le tue risorse AWS tramite browser Web, applicazioni client, app mobili o strumenti a 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 per leggere i dati. Queste identità includono macchine in esecuzione nell'ambiente AWS, ad esempio istanze Amazon EC2 o funzioni AWS Lambda. Puoi anche gestire le identità di macchine per soggetti esterni che necessitano dell'accesso. Inoltre, potresti disporre di macchine al di fuori di AWS che devono accedere al tuo ambiente AWS.

Best practice

- [SEC02-BP01 Utilizzo 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 provider di identità centralizzato](#)
- [SEC02-BP05 Verifica e rotazione periodica delle credenziali](#)

- [SEC02-BP06 Utilizzo dei gruppi di utenti e degli attributi](#)

SEC02-BP01 Utilizzo meccanismi di accesso efficaci

I sign-in (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 questi rischi, richiedendo l'MFA e policy sulle password sicure.

Risultato desiderato: ridurre i rischi di accesso involontario alle credenziali in AWS utilizzando meccanismi di accesso efficaci per gli utenti [AWS Identity and Access Management \(IAM\)](#), l'[utente root Account AWS](#), [AWS IAM Identity Center](#) (successore di AWS Single Sign-On) e i provider di identità 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 molti modi in cui le identità umane possono accedere ad AWS. È una best practice di AWS affidarsi a un provider di identità centralizzato che si avvale della federazione (federazione diretta o utilizzo di AWS IAM Identity Center) per l'autenticazione ad AWS. In questo caso, è necessario stabilire un processo di accesso sicuro con il provider di identità o con Microsoft Active Directory.

Quando apri un Account AWS, inizi con un utente root Account AWS. L'account utente root deve essere utilizzato solo per impostare l'accesso per gli utenti e per le [attività che richiedono l'utente root](#). È importante abilitare l'MFA per l'utente root dell'account subito dopo l'apertura di Account AWS e proteggere l'utente root usando la guida AWS alle [best practice](#).

Se crei utenti in AWS IAM Identity Center, proteggi il processo di accesso in quel servizio. Per le identità dei consumatori, puoi usare [Amazon Cognito user pools](#) e proteggere il processo di accesso

in tale servizio oppure puoi utilizzare uno dei fornitori di identità supportato da Amazon Cognito user pools.

Se si utilizzano gli utenti [AWS Identity and Access Management \(IAM\)](#), è opportuno proteggere il processo di accesso mediante IAM.

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

Passaggi dell'implementazione

Le seguenti sono raccomandazioni generali per l'accesso sicuro. Le impostazioni effettive da configurare devono essere stabilite dalla policy aziendale o utilizzare uno standard come [NIST 800-63](#).

- Richiedere l'MFA. [Richiedere l'MFA è una best practice IAM](#) per le identità e i carichi di lavoro umani. L'abilitazione 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 crittograficamente da un dispositivo hardware.
- Applicare una lunghezza minima della password, che è un fattore primario nella forza della password.
- Applicare la complessità delle password in modo che sia più difficile individuarle.
- Consentire agli utenti di modificare le proprie password.
- Creare identità individuali invece di credenziali condivise. Creando identità individuali, è possibile assegnare a ciascun utente un set unico di credenziali di sicurezza. I singoli utenti consentono di sottoporre a audit l'attività di ciascuno.

Suggerimenti IAM Identity Center:

- IAM Identity Center fornisce una [policy sulla password](#) prestabilita quando si utilizza la directory predefinita che stabilisce i requisiti di lunghezza, complessità e riutilizzo delle password.
- [Abilitare l'MFA](#) e configurare l'impostazione "Compatibile con il contesto" o "Sempre attivo" per l'MFA quando l'origine dell'identità è la directory predefinita, AWS Managed Microsoft AD o AD Connector.
- Consenti agli utenti di [registrare i propri dispositivi MFA](#).

Suggerimenti sulla directory Amazon Cognito user pools:

- Configura le impostazioni di [forza della password](#).
- [Richiedi l'MFA](#) per gli utenti.
- Utilizza le Amazon Cognito user pools [impostazioni di sicurezza avanzate](#) per le funzionalità quali [l'autenticazione adattiva](#) che può bloccare sign-in sospetti.

Suggerimenti per l'utente IAM:

- Idealmente stai utilizzando IAM Identity Center o la federazione diretta. Tuttavia, potrebbero essere necessari utenti IAM. In tal caso, [imposta una policy sulla password](#) per gli utenti IAM. Puoi utilizzare la policy sulla 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 modo che gli utenti possano gestire le proprie password e i dispositivi MFA.

Risorse

Best practice correlate:

- [SEC02-BP03 Archiviazione e utilizzo dei segreti in modo sicuro](#)
- [SEC02-BP04 Fai affidamento su un provider di identità centralizzato](#)
- [SEC03-BP08 Condivisione delle risorse in modo sicuro all'interno dell'organizzazione](#)

Documenti correlati:

- [AWS IAM Identity Center \(successor to AWS Single Sign-On\) Password Policy](#) Policy sulle password AWS IAM Identity Center (successore di AWS Single Sign-On)
- [IAM user password policy](#) (Policy sulle password degli utenti IAM)
- [Setting the Account AWS root user password](#) (Impostazione della password dell'utente root dell'account AWS)
- [Amazon Cognito password policy](#) (Policy sulla password di Amazon Cognito)
- [AWS credentials](#) (Credenziali AWS)
- [IAM security best practices](#) (Best Practice di sicurezza IAM)

Video correlati:

- [Managing user permissions at scale with AWS IAM Identity Center](#) (Gestire le autorizzazioni degli utenti su larga scala con AWS SSO)
- [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 credenziali.

Risultato desiderato: per ridurre il rischio legato alle credenziali a lungo termine, utilizza credenziali temporanee ogni qualvolta sia possibile sia per le identità umane che per le identità macchina. Le credenziali a lungo termine creano molti rischi, ad esempio possono essere caricate in codice su repository GitHub pubblici. Utilizzando credenziali temporanee, riduci notevolmente le possibilità di compromissione delle credenziali.

Anti-pattern comuni:

- Sviluppatori che utilizzano chiavi di accesso a lungo termine dagli IAM users 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 applicazioni 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 invece di credenziali a lungo termine per tutte le richieste API e CLI AWS. Le richieste API e CLI ai servizi AWS devono, in quasi tutti i casi, essere firmate utilizzando le [chiavi di accesso AWS](#). Queste richieste possono essere firmate con credenziali

temporanee o a lungo termine. L'unico caso in cui si devono utilizzare credenziali a lungo termine, note anche come chiavi di accesso a lungo termine, è qualora si stia utilizzando un [utente IAM](#) o un [utente root Account AWS](#). Al momento della federazione ad AWS o dell'assunzione di un [ruolo IAM](#) attraverso altri metodi, vengono generate delle credenziali temporanee. Anche quando accedi a AWS Management Console utilizzando le credenziali di accesso, vengono generate credenziali temporanee per effettuare chiamate ai servizi AWS. Sono poche le situazioni in cui è necessario disporre di 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 in passato gli utenti IAM siano stati utilizzati 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

Per le identità umane come dipendenti, amministratori, sviluppatori, operatori e clienti:

- Devi [affidarti a un fornitore di identità centralizzato](#) e [richiedere agli utenti umani di utilizzare la federazione con un fornitore di identità per accedere ad AWS utilizzando credenziali temporanee](#). La federazione degli utenti può essere effettuata con [la federazione diretta a ciascun Account AWS](#) o utilizzando [AWS IAM Identity Center \(successore di AWS IAM Identity Center\)](#) e un provider di identità a scelta. La federazione offre una serie di vantaggi rispetto all'utilizzo degli utenti IAM, oltre all'eliminazione delle credenziali a lungo termine. Gli utenti possono anche richiedere credenziali temporanee dalla riga di comando per la [federazione diretta](#) o utilizzare [IAM Identity Center](#). Ciò significa che i casi d'uso che richiedono utenti IAM o credenziali a lungo termine per gli utenti sono pochi.
- Quando concedi a terzi, come ad esempio ai fornitori di software come servizio (SaaS), l'accesso alle risorse del tuo Account AWS, puoi utilizzare [ruoli multi-account](#) e [policy basate sulle risorse](#).
- Se devi concedere l'accesso alle tue risorse alle applicazioni per i consumatori o per i clienti AWS, puoi utilizzare i [pool di identità Amazon Cognito](#) o [Amazon Cognito user pools](#) per fornire le credenziali temporanee. Le autorizzazioni per le credenziali sono configurate tramite i ruoli IAM. Puoi anche definire un ruolo IAM separato con autorizzazioni limitate per gli utenti guest non autenticati.

Per le identità macchina, potrebbero essere necessarie credenziali a lungo termine. In questi casi, devi [richiedere ai carichi di lavoro di utilizzare credenziali temporanee con ruoli IAM per accedere ad AWS](#).

- Per [Amazon Elastic Compute Cloud](#) (Amazon EC2), puoi utilizzare [ruoli per Amazon EC2](#).
- [AWS Lambda](#) ti consente di configurare un [ruolo di esecuzione Lambda per concedere le autorizzazioni al servizio](#) per eseguire azioni AWS utilizzando credenziali temporanee. Per i servizi AWS esistono molti altri modelli simili per concedere credenziali temporanee utilizzando i ruoli IAM.
- Per i dispositivi IoT, puoi utilizzare il [provider di credenziali AWS IoT Core](#) per richiedere credenziali temporanee.
- Per i sistemi on-premise o per i sistemi che vengono eseguiti al di fuori di AWS che richiedono accesso alle risorse AWS, puoi utilizzare [IAM Roles Anywhere](#).

Esistono scenari in cui le credenziali temporanee non sono un'opzione e potrebbe essere necessario utilizzare credenziali a lungo termine. In queste situazioni, [sottoporti a audit e ruota periodicamente le credenziali](#) e [ruota regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine](#). Alcuni esempi che potrebbero richiedere credenziali a lungo termine sono i plugin di WordPress e i client AWS di terze parti. Quando è necessario utilizzare credenziali a lungo termine o per credenziali diverse dalle chiavi di accesso AWS, come ad esempio i login ai database, puoi utilizzare un servizio progettato per gestire i segreti, ad esempio [AWS Secrets Manager](#). Secrets Manager consente di gestire, ruotare e archiviare in modo semplice e sicuro i segreti crittografati usando [servizi supportati](#). Per ulteriori informazioni sulla rotazione delle credenziali a lungo termine, consulta [Rotating Access Keys](#) (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 provider di identità centralizzato](#)
- [SEC03-BP08 Condivisione delle risorse in modo sicuro all'interno dell'organizzazione](#)

Documenti correlati:

- [Credenziali di sicurezza temporanee](#)

- [AWS Credentials](#) (Credenziali AWS)
- [IAM Security Best Practices](#) (Best practice per la sicurezza IAM)
- [Ruoli IAM](#)
- [IAM Identity Center](#)
- [Provider di identità e federazione](#)
- [Rotating Access Keys](#)
- [Soluzioni dei partner per la sicurezza: accesso e controllo degli accessi](#)
- [L'utente root dell'account AWS](#)

Video correlati:

- [Managing user permissions at scale with AWS IAM Identity Center \(Gestire le autorizzazioni degli utenti su larga scala con AWS SSO\), successore di 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: implementare un meccanismo per la gestione sicura delle credenziali delle applicazioni che raggiunga 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, quando 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 regolato da un'API (si pensi a un distributore automatico di credenziali).
- L'accesso a una credenziale (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 separato dal resto dell'architettura.
- I segreti vengono distribuiti automaticamente su richiesta ai componenti software e la rotazione avviene in una posizione centrale.
- L'accesso alle credenziali può essere controllato 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 automaticamente e sottoporre a audit il loro utilizzo.

Il modo migliore per affrontare la gestione dei segreti è seguire le indicazioni di rimuovere, sostituire e ruotare. La credenziale più sicura è quella che non si deve memorizzare, gestire o trattare. Possono esserci credenziali che non sono più necessarie per il funzionamento del carico di lavoro e che possono essere rimosse in modo sicuro.

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

Alcuni segreti di lunga durata potrebbero non poter essere rimossi o sostituiti. Questi segreti possono essere memorizzati in un servizio come [AWS Secrets Manager](#), dove possono essere archiviati, gestiti e ruotati regolarmente a livello centrale.

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:

Credential type	Description	Suggested strategy
IAM access keys	AWS IAM access and secret keys used to assume IAM roles inside of a workload	Replace: Use Ruoli IAM assigned to the compute instances (such as Amazon EC2 or AWS Lambda) instead. For interoperability with third parties that require access to resources in your Account AWS, ask if they support AWS cross-account access (Accesso multi-account AWS). For mobile apps, consider using temporary credentials through Pool di identità di Amazon Cognito (identità federate) . For workloads running outside of AWS, consider IAM Roles Anywhere or Attivazioni ibride AWS Systems Manager .
SSH keys	Secure Shell private keys used to log into Linux EC2 instances, manually or as part of an automated process	Replace: Use AWS Systems Manager or EC2 Instance Connect to provide programmatic and human access to EC2 instances using IAM roles.
Application and database credentials	Passwords – plain text string	Rotate: Store credentials in AWS Secrets Manager and

Credential type	Description	Suggested strategy
		establish automated rotation if possible.
Amazon RDS and Aurora Admin Database credentials	Passwords – plain text string	Replace: Use the Secrets Manager integration with Amazon RDS (Integrazione di Secrets Manager con Amazon RDS) or Amazon Aurora . In addition, some RDS database types can use IAM roles instead of passwords for some use cases (for more detail, see IAM database authentication (Autenticazione del database IAM)).
OAuth tokens	Secret tokens – plain text string	Rotate: Store tokens in AWS Secrets Manager and configure automated rotation.
API tokens and keys	Secret tokens – plain text string	Rotate: Store in AWS Secrets Manager and establish automated rotation if possible.

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. Quando è richiesta una chiave di accesso IAM per comunicare con un servizio AWS, utilizza le [credenziali di sicurezza temporanee \(a breve termine\)](#). Queste credenziali a breve termine possono essere fornite attraverso [ruoli IAM per istanze EC2](#), [ruoli di esecuzione](#) per funzioni Lambda, [ruoli Cognito IAM](#) per l'accesso degli utenti di dispositivi mobili e [policy IoT Core](#) per i dispositivi IoT. Quando ci si interfaccia con terze parti, è preferibile [delegare l'accesso a un ruolo IAM](#) con l'accesso necessario alle risorse del proprio account, piuttosto che configurare un utente IAM e inviare alla terza parte la chiave di accesso segreta per quell'utente.

In molti casi il carico di lavoro richiede la memorizzazione di segreti necessari per l'interoperabilità con altri servizi e risorse. [AWS Secrets Manager](#) è costruito appositamente per gestire in modo sicuro queste credenziali, nonché l'archiviazione, l'uso e la rotazione di token API, password e altre credenziali.

AWS Secrets Manager fornisce cinque funzionalità chiave per garantire l'archiviazione e la gestione sicura delle credenziali sensibili: [crittografia a riposo](#), [crittografia in transito](#), [audit completo](#), [controllo degli accessi granulare](#) e [rotazione estensibile delle credenziali](#). Sono accettabili anche altri servizi di gestione dei segreti dei partner AWS o soluzioni sviluppate localmente che forniscano funzionalità e garanzie simili.

Passaggi dell'implementazione

1. Individuare i percorsi di codice contenenti credenziali hard-coded utilizzando strumenti automatizzati come [Amazon CodeGuru](#).
 - Utilizzare Amazon CodeGuru per eseguire la scansione dei repository di codice. Una volta completata la revisione, filtrare Type=Secrets in CodeGuru per trovare le linee di codice problematiche.
2. Identificare le credenziali che possono essere rimosse o sostituite.
 - a. Identificare 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 una parte del carico di lavoro è al di fuori di AWS ma richiede le credenziali IAM per accedere alle risorse AWS, considerare [IAM Roles Anywhere](#) o [Attivazioni ibride AWS Systems Manager](#).
3. Per altri segreti di terze parti a lunga durata che richiedono l'uso della strategia di rotazione, integrare Secrets Manager nel codice per recuperare i segreti di terze parti in fase di esecuzione.
 - a. La console CodeGuru può [creare un segreto in Secrets Manager](#) automaticamente utilizzando le credenziali individuate.
 - b. Integrare il recupero dei segreti da Secrets Manager nel codice dell'applicazione.
 - Le funzioni Lambda serverless possono utilizzare un'[estensione Lambda](#) indipendente dal linguaggio.
 - Per le istanze o i container EC2, AWS fornisce esempi di [codice lato client per il recupero dei segreti da Secrets Manager](#) in diversi linguaggi di programmazione popolari.
4. Esaminare periodicamente la base di codice e ripetere la scansione per verificare che non siano stati aggiunti nuovi segreti al codice.

- Valutare l'utilizzo di uno strumento come [git-secrets](#) per impedire il commit di nuovi segreti nel repository del codice sorgente.
5. [Monitorare l'attività di Secrets Manager](#) per rilevare indicazioni di utilizzo inatteso, accesso inappropriato ai segreti o tentativi di cancellazione dei segreti.
 6. Ridurre l'esposizione umana alle credenziali. Limitare l'accesso alle credenziali di lettura, scrittura e modifica a un ruolo IAM dedicato a questo scopo e fornire l'accesso per assumere il ruolo solo a 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 AWS Secrets Manager](#)
- [Provider di identità e federazione](#)
- [Amazon CodeGuru Introduces Secrets Detector](#) (Amazon CodeGuru introduce il rivelatore di segreti)
- [How AWS Secrets Manager uses AWS Key Management Service](#) (In che modo AWS Secrets Manager utilizza AWS Key Management Service)
- [Crittografia e decrittografia del segreto in Secrets Manager](#)
- [Articoli del blog su Secrets Manager](#)
- [Amazon RDS announces integration with AWS Secrets Manager](#) (Amazon RDS announces integration with AWS Secrets Manager)

Video correlati:

- [Best practice per la gestione, il recupero e la rotazione di segreti su scala](#)
- [Find Hard-Coded Secrets Using Amazon CodeGuru Secrets Detector](#) (Trovare i segreti codificati usando il rilevatore di segreti di Amazon CodeGuru)

- [Securing Secrets for Hybrid Workloads Using AWS Secrets Manager](#) (Trovare i segreti codificati usando il rilevatore di segreti di Amazon CodeGuru)

Workshop correlati:

- [Store, retrieve, and manage sensitive credentials in AWS Secrets Manager](#) (Memorizzare, recuperare e gestire le credenziali sensibili in AWS Secrets Manager)
- [Attivazioni ibride AWS Systems Manager](#)

SEC02-BP04 Fai affidamento su un provider di identità centralizzato

Per le identità della forza lavoro (dipendenti e collaboratori) affidati a un provider di 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, perché crei, assegni, gestisci, revochi e verifichi gli accessi da una singola posizione.

Risultato desiderato: Hai un provider di identità centralizzato dal quale gestisci centralmente gli utenti della forza lavoro, le policy di autenticazione (come le richieste di autenticazione a più fattori o 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 provider di identità 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 provider di identità è integrato con i tuoi sistemi di risorse umane (HR), in modo che le modifiche relative al personale vengano sincronizzate automaticamente con il provider di identità. 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 provider di identità e stai monitorando questi log per rilevare comportamenti degli utenti insoliti.

Anti-pattern comuni:

- Non utilizzi la federazione e l'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 provider di identità 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 provider di identità centralizzato ti fornisce un unico posto 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 la possibilità 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 provider di identità e le applicazioni e le autorizzazioni assegnate vengono aggiornate automaticamente. Quando un utente lascia l'organizzazione, la sua identità viene automaticamente disabilitata nel provider di identità 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

Linee guida per l'accesso ad AWS degli utenti che fanno parte della forza lavoro

Gli utenti che fanno parte della forza lavoro, come dipendenti e collaboratori dell'organizzazione, potrebbero richiedere l'accesso ad AWS per utilizzare la AWS Management Console o la AWS Command Line Interface (AWS CLI) per svolgere le proprie mansioni lavorative. Puoi concedere l'accesso ad AWS a tali utenti federando il tuo provider di identità 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 ciascuno Account AWS, utilizza un provider di identità centralizzato per federare l'accesso a [AWS Identity and Access Management](#) in quell'account. Grazie alla sua flessibilità, IAM ti permette di abilitare un [SAML 2.0](#) o un [Open ID Connect \(OIDC\)](#) Identity Provider per ciascun Account AWS e di utilizzare attributi utente federati per il controllo degli accessi. Gli utenti della tua forza lavoro utilizzano il proprio browser Web per accedere al provider di identità e forniscono le proprie credenziali (come password e codici token MFA). Il provider di identità rilascia un'asserzione SAML nel browser che viene inviata all'URL di accesso della AWS Management Console, così da consentire all'utente di accedere mediante l'autenticazione unica alla [AWS Management Console tramite l'assunzione di un ruolo IAM](#). Gli utenti possono anche ottenere credenziali API AWS temporanee da utilizzare nella [AWS CLI](#) o [AWS SDK](#) da [AWS STS](#) tramite [l'assunzione del ruolo IAM utilizzando un'asserzione SAML](#) ottenuta dal provider di identità.
- Per federare gli utenti della tua forza lavoro con più account all'interno dell'organizzazione AWS, puoi usare [AWS IAM Identity Center](#) per gestire centralmente l'accesso degli utenti agli Account AWS e alle applicazioni. Attiva Centro di identità per la tua organizzazione e configura la tua origine di identità. IAM Identity Center fornisce una directory di origine delle identità predefinita,

che puoi utilizzare per gestire utenti e gruppi. In alternativa, puoi scegliere un'origine di identità esterna [connettendoti al tuo provider di identità esterno](#) tramite SAML 2.0 ed [effettuando il provisioning automatico](#) di utenti e gruppi che utilizzano SCIM, oppure [connettendoti a Microsoft AD Directory](#) utilizzando [AWS 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 nel tuo [set di autorizzazioni](#). Gli utenti della tua forza lavoro possono autenticarsi tramite il provider di identità centrale per accedere al [portale di accesso AWS](#) ed effettuare l'autenticazione unica per ottenere l'accesso agli Account AWS e alle applicazioni cloud a loro assegnate. Gli utenti possono configurare [AWS CLI v2](#) per autenticarsi con Centro di identità e ottenere le credenziali per eseguire comandi della AWS CLI. Centro di identità consente inoltre l'accesso tramite autenticazione unica ad applicazioni AWS come [Amazon SageMaker Studio](#) e [ai portali AWS IoT SiteWise Monitor](#).

Dopo aver seguito le indicazioni precedenti, gli utenti della forza lavoro non avranno più bisogno di utilizzare IAM users e gruppi per le normali operazioni quando gestiscono i carichi di lavoro su AWS. Al contrario, gli utenti e i gruppi sono gestiti all'esterno di AWS e gli utenti possono accedere alle risorse AWS come identità federata. Le identità federate utilizzano i gruppi definiti dal provider di identità centralizzato. Devi identificare e rimuovere i gruppi IAM, gli IAM users e le credenziali utente di lunga durata (password e chiavi di accesso) che non sono più necessarie nei tuoi Account AWS. Puoi [trovare credenziali inutilizzate](#) utilizzando [il report sulle credenziali IAM](#), [eliminare gli IAM users interessati](#) e [rimuovere i gruppi IAM](#). Puoi applicare una [policy di controllo dei servizi \(SCP\)](#) alla tua organizzazione per prevenire la creazione di nuovi IAM users e gruppi, applicando l'accesso ad AWS tramite identità federate.

Linee guida per gli utenti delle tue applicazioni

Puoi gestire le identità degli utenti delle applicazioni, ad esempio un'app per dispositivi mobili, utilizzando [Amazon Cognito](#) come provider di identità centralizzato. Amazon Cognito consente l'autenticazione, l'autorizzazione e la gestione degli utenti per le app Web e mobili. Amazon Cognito fornisce un archivio di identità dimensionabile fino a milioni di utenti, supporta la federazione delle identità sociali e aziendali e offre funzionalità di sicurezza avanzate per proteggere gli utenti e l'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

Procedure per l'accesso ad AWS degli utenti che fanno parte della forza lavoro

- Federa l'accesso ad AWS degli utenti della tua forza lavoro tramite un provider di identità centralizzato seguendo uno dei seguenti approcci:
 - Utilizza IAM Identity Center per abilitare l'autenticazione unica negli Account AWS per più utenti della tua organizzazione AWS tramite la federazione con il provider di identità.
 - Utilizza IAM per connettere il provider di identità direttamente a ciascun Account AWS, abilitando un accesso federato e granulare.
- Identifica e rimuovi gli IAM users e i gruppi che vengono sostituiti da identità federate.

Passaggi per gli utenti delle tue applicazioni

- Utilizza Amazon Cognito come provider di identità centralizzato per le tue applicazioni.
- Integra le applicazioni personalizzate con Amazon Cognito utilizzando 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 Well-Architected correlate:

- [SEC02-BP06 Utilizzo 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:

- [Identity federation in AWS](#)
- [Best practice per la sicurezza in IAM](#)
- [AWS Identity and Access Management Best practices](#)
- [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: IAM Identity Center credential provider](#)

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](#)
- [Workshop: Serverless identity](#)

Strumenti correlati:

- [Partner AWS 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 accedere alle risorse. Le credenziali a lungo termine espongono a molti rischi che possono essere ridotti ruotandole regolarmente.

Risultato desiderato: implementare la rotazione delle credenziali per ridurre i rischi associati all'utilizzo 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: medio

Guida all'implementazione

Quando non si può fare affidamento sulle credenziali temporanee e sono necessarie credenziali a lungo termine, sottoponile a audit per assicurarti che siano applicati i controlli prestabiliti, ad esempio l'autenticazione a più fattori (MFA), che siano soggette a regolare rotazione e dispongano di un livello di accesso appropriato.

La convalida periodica, preferibilmente tramite uno strumento automatizzato, è necessaria per verificare che vengano applicati i 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. Quando passi da utenti AWS Identity and Access Management (IAM) a identità centralizzate, puoi [generare un report delle credenziali](#) per effettuare l'audit degli utenti.

Ti consigliamo inoltre di monitorare l'MFA nel tuo provider di identità. Puoi configurare [Regole di AWS Config](#) o utilizzare gli [standard di sicurezza AWS Security Hub](#) per verificare se gli utenti hanno l'MFA abilitata. Considera 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, è necessario un audit frequente e la rotazione delle chiavi di accesso.

Passaggi dell'implementazione

- Eseguire regolarmente l'audit delle credenziali: l'audit delle identità configurate nel provider di identità e in IAM aiuta a verificare che solo le identità autorizzate abbiano accesso al carico di lavoro. Tali identità possono includere, a titolo esemplificativo ma non esaustivo, utenti IAM, utenti AWS IAM Identity Center, utenti Active Directory o utenti in un diverso provider di identità a monte. Ad esempio, eliminare le persone che lasciano l'organizzazione e i ruoli multi-account che non sono più necessari. Disporre di un processo per sottoporre periodicamente a audit le autorizzazioni ai servizi a cui accede un'entità IAM. Questo aiuta a 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 autorizzazioni e credenziali IAM. Puoi utilizzare [Amazon CloudWatch per configurare allarmi per chiamate API specifiche](#) effettuate nell'ambiente AWS. [Amazon GuardDuty può anche avvisare di attività impreviste](#), che potrebbero indicare un accesso estremamente permissivo o un accesso non intenzionale alle credenziali IAM.
- Ruota regolarmente le credenziali: quando non è possibile utilizzare le credenziali temporanee, ruotare regolarmente le chiavi di accesso IAM a lungo termine, al massimo ogni 90 giorni. Se una chiave di accesso viene involontariamente divulgata a propria insaputa, 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 [Rotating access keys](#).

- Rivedi le autorizzazioni IAM: per migliorare la sicurezza dell'Account AWS, rivedere e monitorare regolarmente ogni policy IAM. Verifica che le policy rispettino il principio del privilegio minimo.
- Considera la possibilità di automatizzare la creazione e gli aggiornamenti delle risorse IAM: IAM Identity Center automatizza molte attività IAM, come la gestione dei ruoli e delle 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.
- Utilizza IAM Roles Anywhere per sostituire gli utenti IAM per le identità macchina: IAM Roles Anywhere consente di utilizzare i ruoli in aree tradizionalmente non accessibili, come i server on-premise. IAM Roles Anywhere utilizza un certificato X.509 affidabile per autenticarsi ad AWS e ricevere 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-premise. 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 AWS Secrets Manager](#)
- [IAM Best Practices](#)(Best Practice IAM)
- [Provider di identità e federazione](#)
- [Soluzioni dei partner per la sicurezza: accesso e controllo degli accessi](#)
- [Credenziali di sicurezza temporanee](#)
- [Recupero dei report delle credenziali per l'Account AWS](#)

Video correlati:

- [Best practice per la gestione, il recupero e la rotazione di segreti su scala](#)

- [Managing user permissions at scale with AWS IAM Identity Center](#) (Gestire le autorizzazioni degli utenti su larga scala con AWS SSO)
- [Mastering identity at every layer of the cake](#)

Esempi correlati:

- [Well-Architected Lab - Automated IAM User Cleanup](#) (Well-Architected Lab - Pulizia automatica degli utenti IAM)
- [Well-Architected Lab - Automated Deployment of IAM Groups and Roles](#) (Well-Architected Lab - Distribuzione automatica di gruppi e ruoli IAM)

SEC02-BP06 Utilizzo dei gruppi di utenti e degli attributi

Man mano che il numero di utenti gestiti cresce, sarà necessario determinare i modi per organizzarli in modo da poterli gestire su vasta scala. Inserisci gli utenti con requisiti di sicurezza comuni in gruppi definiti dal provider di identità e metti in atto meccanismi per garantire che gli attributi utente che potrebbero essere utilizzati per il controllo degli accessi (ad esempio, reparto o posizione) siano corretti e aggiornati. Utilizza questi gruppi e attributi, anziché i singoli utenti, per controllare l'accesso. In questo modo puoi gestire l'accesso centralmente, modificando una volta sola l'appartenenza o gli attributi di un gruppo utente con un [set di autorizzazioni](#), anziché aggiornare numerose policy individuali quando le esigenze di accesso di un utente cambiano. Puoi utilizzare AWS IAM Identity Center (IAM Identity Center) per gestire gruppi di utenti e attributi. IAM Identity Center supporta la maggior parte degli attributi utilizzati, indipendentemente dal fatto che vengano inseriti manualmente durante la creazione dell'utente o assegnati automaticamente utilizzando un motore di sincronizzazione, come definito nella specifica System for Cross-Domain Identity Management (SCIM).

Inserisci gli utenti con requisiti di sicurezza comuni in gruppi definiti dal provider di identità e metti in atto meccanismi per garantire che gli attributi utente che potrebbero essere utilizzati per il controllo degli accessi (ad esempio, reparto o posizione) siano corretti e aggiornati. Utilizza questi gruppi e attributi, anziché i singoli utenti, per controllare l'accesso. In questo modo è possibile gestire l'accesso centralmente, modificando una volta sola l'appartenenza o gli attributi di un gruppo utente, anziché aggiornare numerose policy individuali quando le esigenze di accesso di un utente cambiano.

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

Guida all'implementazione

- Se stai utilizzando AWS IAM Identity Center (IAM Identity Center), configura i gruppi: IAM Identity Center offre la possibilità di configurare gruppi di utenti e di assegnare ai gruppi il livello di autorizzazione desiderato.
 - [AWS Single Sign-On - Gestione delle identità](#)
- Scopri il controllo degli accessi basato su attributi (ABAC): ABAC è una strategia di autorizzazione che definisce i permessi in base agli attributi.
 - [Che cos'è ABAC per AWS?](#)
 - [Laboratorio: controllo degli accessi basato su tag IAM per EC2](#)

Risorse

Documenti correlati:

- [Nozioni di base su AWS Secrets Manager](#)
- [Best practice IAM](#)
- [Provider di identità e federazione](#)
- [L'utente root dell'account AWS](#)

Video correlati:

- [Best practice per la gestione, il recupero e la rotazione di segreti su scala](#)
- [Gestione delle autorizzazioni utente su scala con AWS IAM Identity Center](#)
- [Mastering identity at every layer of the cake](#)

Esempi correlati:

- [Laboratorio: controllo degli accessi basato su tag IAM per EC2](#)

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 controllano chi può accedere a cosa e a quali condizioni. Imposta le autorizzazioni per specifiche identità umane e di macchine per

concedere l'accesso a determinate azioni del servizio su risorse specifiche. Inoltre, specifica le condizioni che devono essere vere per concedere l'accesso. Ad esempio, puoi consentire agli sviluppatori di creare nuove funzioni Lambda, ma solo in una regione specifica. Quando gestisci gli ambienti AWS su vasta scala, attieniti alle seguenti best practice per garantire che le identità abbiano solo l'accesso necessario e nient'altro.

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

[Policy basate sulle identità](#) in IAM sono gestite o inline e collegate a identità IAM, inclusi utenti, gruppi o ruoli. Queste policy ti permettono di specificare cosa può fare l'identità (le sue autorizzazioni). Le policy basate sulle identità possono essere ulteriormente categorizzate.

Policy gestite: policy standalone basate su identità che puoi collegare a più utenti, gruppi e ruoli nel tuo account AWS. Esistono due tipi di policy gestite:

- Policy gestite AWS: policy gestite create e gestite da AWS.
- Policy gestite dal cliente: policy gestite che crei e gestisci nel tuo 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 mantengono una relazione rigida una a una tra una policy e un'identità. Le policy inline vengono eliminate quando elimini l'identità.

Nella maggior parte dei casi, dovresti creare le policy gestite dal cliente proprietarie seguendo il principio del [privilegio minimo](#).

Le [policy basate sulle 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 policy basate sulle risorse, consulta [Servizi AWS che funzionano con IAM](#).

I [limiti delle autorizzazioni](#) usano una policy gestita per definire 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.

[Controllo degli accessi basato su attributi \(ABAC\)](#) consente di concedere autorizzazioni in base agli attributi. In AWS, questi sono denominati tag. I tag possono essere collegati ai principali IAM (utenti o ruoli) e alle risorse AWS. Utilizzando le policy IAM, gli amministratori possono creare una policy riutilizzabile che applica 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 degli sviluppatori. Man mano che il team di sviluppatori aggiunge risorse ai progetti, le autorizzazioni vengono applicate automaticamente in base agli attributi. Di conseguenza, non è richiesto alcun aggiornamento delle policy per ogni nuova risorsa.

Le [policy di controllo del servizio \(SCP\) di Organizations](#) definiscono il limite massimo di autorizzazioni per i membri dell'account di un'organizzazione o unità organizzativa (UO). Le SCP limitano le autorizzazioni che le policy basate su identità o risorse concedono alle entità (utenti o ruoli) all'interno dell'account ma non concedono autorizzazioni.

Le [policy di sessione](#) assumono 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. Queste policy limitano le autorizzazioni per una sessione creata, ma non concedono autorizzazioni. Per ulteriori informazioni, consulta [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 pubblico e multi-account](#)
- [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. Individua una definizione chiara di chi o cosa deve avere accesso a ciascun componente, quindi 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: alto

Guida all'implementazione

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

L'accesso regolare agli Account AWS dell'organizzazione viene fornito utilizzando [l'accesso federato](#) o un gestore dell'identità 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, quando 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.

Quando si definiscono i requisiti di accesso per le identità non umane, determina quali applicazioni e componenti devono accedere e come vengono concesse le autorizzazioni. L'utilizzo di ruoli IAM creati con il modello di accesso con privilegi minimi è un approccio consigliato. [Le policy gestite da AWS](#) forniscono le policy IAM predefinite che coprono la maggior parte dei casi d'uso comuni.

I servizi AWS, come [AWS Secrets Manager](#) e [Archivio dei parametri AWS Systems Manager](#) consentono di scollegare i segreti dall'applicazione o dal carico di lavoro in modo sicuro nei casi in cui non è possibile utilizzare i ruoli IAM. 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 usare AWS Identity and Access Management Roles Anywhere per ottenere [credenziali di sicurezza temporanee in IAM](#) per i carichi di lavoro eseguiti all'esterno di AWS. I tuoi carichi di lavoro possono utilizzare le stesse [policy IAM](#) e [ruoli IAM](#) che usi 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 gli utenti IAM devono avere l'accesso programmatico e credenziali a lungo termine, utilizza [le ultime informazioni usate per la chiave di accesso](#) per ruotare e rimuovere le chiavi di accesso.

Risorse

Documenti correlati:

- [Il controllo dell'accesso basato su attributi \(Attribute-Based Access Control, ABAC\)](#)
- [AWS IAM Identity Center](#)
- [IAM Roles Anywhere](#)
- [AWS Managed policies for IAM Identity Center \(Policy gestite da AWS per IAM Identity Center\)](#)
- [AWS IAM policy conditions \(Condizioni delle policy AWS IAM\)](#)
- [Casi d'uso IAM](#)
- [Rimozione di credenziali non necessarie](#)
- [Lavorare con le policy](#)
- [How to control access to AWS resources based on Account AWS, OU, or organization \(Come controllare l'accesso alle risorse AWS in base all'account, all'unità organizzativa o all'organizzazione AWS\)](#)
- [Identify, arrange, and manage secrets easily using enhanced search in AWS Secrets Manager \(Identificazione, organizzazione e gestione semplificate dei segreti con la ricerca avanzata di AWS Secrets Manager\)](#)

Video correlati:

- [Become an IAM Policy Master in 60 Minutes or Less \(Diventa un IAM Policy Master in 60 minuti\)](#)
- [Separation of Duties, Least Privilege, Delegation, and CI/CD \(Separazione dei compiti, privilegio minimo, delega e integrazione e distribuzione continua \(CI/CD\)\)](#)
- [Streamlining identity and access management for innovation \(Semplificazione della gestione delle identità e degli accessi per l'innovazione\)](#)

SEC03-BP02 Concessione dell'accesso con privilegio minimo

È una best practice concedere alle identità soltanto il livello di accesso di cui hanno bisogno, specificando le operazioni che possono effettuare, le risorse su cui possono operare e a quali condizioni. Affidati ai gruppi e agli attributi di identità per impostare dinamicamente 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, il suo accesso viene automaticamente revocato senza modificare le policy di accesso sottostanti.

Risultato desiderato: gli utenti devono avere solo le autorizzazioni necessarie per portare a termine la loro attività. Gli utenti dovrebbero avere accesso solo agli ambienti di produzione per eseguire un'attività specifica in un intervallo temporale limitato e l'accesso dovrebbe essere revocato una volta completata l'attività. Le autorizzazioni devono essere revocate quando non sono più necessarie, incluso quando un utente passa a un progetto o a un ruolo professionale diversi. I privilegi di amministratore devono essere riservati a un piccolo gruppo di amministratori fidati. Le autorizzazioni devono essere riviste con regolarità per evitare che si accumulino. Account di sistemi o di macchine devono avere il numero minimo di autorizzazioni necessarie per portare a termine un'attività.

Anti-pattern comuni:

- L'impostazione predefinita è la concessione delle autorizzazioni di amministratore agli utenti.
- L'utilizzo dell'utente root per le attività quotidiane.
- Creazione di policy eccessivamente permissive, ma senza privilegi completi di amministratore.
- La mancata revisione delle autorizzazioni per capire se consentono l'accesso privilegio minimo.

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 consentite solo per eseguire il numero minimo di azioni necessarie per completare 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. Gli utenti e i ruoli IAM non hanno autorizzazioni per impostazione predefinita. L'utente root ha accesso completo per impostazione predefinita e dovrebbe essere controllato e monitorato con zelo, nonché usato solo per le [attività che richiedono l'accesso root](#).

Le policy IAM sono utilizzate in modo esplicito per concedere 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 e colleghi una policy IAM, puoi specificare le azioni del servizio, le risorse e le condizioni che devono essere vere affinché AWS consenta o neghi l'accesso. AWS supporta una varietà di condizioni che contribuiscono a ridurre l'accesso. Ad esempio, se usi la [chiave di condizione PrincipalOrgID](#), puoi non autorizzare le operazioni se il richiedente non è parte della tua AWS Organization.

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`. Dovresti avere tipi diversi di policy su più livelli per definire un livello di difesa ben radicato e limitare le autorizzazioni complessive dei tuoi utenti. Puoi anche limitare le autorizzazioni che possono essere concesse e a quali condizioni. Ad esempio, puoi consentire ai team delle applicazioni di creare le proprie policy IAM per i sistemi che creano, ma devi anche applicare un [limite delle autorizzazioni](#) per impostare un limite massimo di autorizzazioni che il sistema può ricevere.

Passaggi dell'implementazione

- Implementazione di policy con privilegi minimi: assegna policy di accesso con privilegi minimi a gruppi e ruoli IAM in modo da rispecchiare il ruolo o la funzione dell'utente che hai definito.
 - Policy di base sull'uso delle API: un modo per stabilire le autorizzazioni necessarie consiste nell'analisi dei log AWS CloudTrail. Questa revisione consente di creare autorizzazioni personalizzate in base alle azioni che l'utente deve realmente eseguire in AWS. [IAM Access Analyzer può generare automaticamente una policy IAM basata su attività](#). Puoi usare IAM Access Advisor a livello di account o di organizzazione per [monitorare le ultime informazioni consultate per una policy specifica](#).
- Prendi in considerazione l'uso di [policy gestite da AWS per le funzioni dell'attività](#). Quando inizi a creare policy di autorizzazioni dettagliate, può essere difficile sapere da dove iniziare. AWS ha policy gestite per ruoli professionali comuni, ad esempio contabili, amministratori di database e data scientist. Queste policy possono contribuire a limitare l'accesso degli utenti e, al contempo, definiscono come implementare le policy di privilegio minimo.
- Rimuovi le autorizzazioni superflue: rimuovi le autorizzazioni non necessarie e rivedi quelle eccessivamente permissive. La [generazione di policy di IAM Access Analyzer](#) può essere utile per perfezionare le policy relative alle autorizzazioni.

- Verifica che gli utenti abbiano un accesso limitato agli ambienti di produzione: gli utenti possono accedere agli ambienti di produzione solo se hanno 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.
- Considerazioni sui limiti delle autorizzazioni: un limite delle autorizzazioni è una caratteristica avanzata per utilizzare una policy gestita che imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM. Il limite delle autorizzazioni di un'entità IAM permette di eseguire solo le operazioni consentite dalle policy basate su identità e dai limiti delle autorizzazioni.
- Prendi in considerazione i [tag delle risorse](#) per le autorizzazioni: un modello di controllo degli accessi basato su attributi che usa tag delle risorse ti consente di concedere l'accesso in base a scopo delle risorse, proprietario, ambiente e altri criteri. Ad esempio, puoi usare tag di risorse per diversificare gli ambienti di produzione e sviluppo. Tramite questi tag puoi limitare gli sviluppatori all'ambiente di sviluppo. Abbinando policy su tag e autorizzazioni, puoi ottenere l'accesso a risorse dettagliate senza dover definire policy personalizzate e complesse per ogni funzione professionale.
- Usa [policy di controllo dei servizi](#) per AWS Organizations. Le policy di controllo dei servizi monitorano centralmente il numero massimo di autorizzazioni disponibili per gli account membri della tua organizzazione. È importante notare che le policy di controllo dei servizi consentono di limitare le autorizzazioni dell'utente root negli account membri. Considera anche 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 dell'utente per la tua organizzazione: le policy del ciclo di vita dell'utente definiscono attività da eseguire quando gli utenti eseguono l'onboarding su AWS, cambiano ruolo o ambito professionale o non hanno più bisogno di accedere a AWS. Le revisioni delle autorizzazioni devono essere eseguite in ogni fase del ciclo di vita di un utente per verificare che siano sufficientemente restrittive e per evitare che si accumulino.
- Stabilisci un piano per analizzare le autorizzazioni con regolarità ed eventualmente rimuovere quelle non necessarie: dovresti periodicamente analizzare l'accesso degli utenti per verificare che non abbiano autorizzazioni troppo permissive. [AWS Config](#) e IAM Access Analyzer può essere utile in fase di audit delle autorizzazioni utente.
- Definisci una matrice dei ruoli professionali: una matrice dei ruoli professionali mostra i diversi ruoli e livelli di accesso richiesti all'interno della tua presenza in AWS. Tramite una matrice dei ruoli professionali puoi definire e separare le autorizzazioni in base alle responsabilità degli utenti

all'interno dell'organizzazione. Usa i gruppi invece di applicare le autorizzazioni direttamente ai singoli utenti o ruoli.

Risorse

Documenti correlati:

- [Assegnare il privilegio minimo](#)
- [Limiti delle autorizzazioni per le entità IAM](#)
- [Tecniche per la scrittura di policy IAM con privilegio minimo](#)
- [IAM Access Analyzer semplifica l'implementazione delle autorizzazioni con privilegio minimo generando IAM policy basate sull'attività di accesso](#)
- [Delegare la gestione delle autorizzazioni agli sviluppatori tramite i limiti delle autorizzazioni IAM](#)
- [Perfezionamento delle autorizzazioni in AWS utilizzando le informazioni sull'ultimo accesso](#)
- [Tipi di policy IAM e quando utilizzarle](#)
- [Test delle policy IAM con il simulatore di policy IAM](#)
- [Guardrail in AWS Control Tower](#)
- [Architetture Zero Trust: una prospettiva AWS](#)
- [Come implementare il principio del privilegio minimo con CloudFormation StackSets](#)
- [Il controllo dell'accesso basato su attributi \(Attribute-Based Access Control, ABAC\)](#)
- [Riduzione dell'ambito di applicazione della policy mediante visualizzazione dell'attività dell'utente](#)
- [Visualizzazione dell'accesso al ruolo](#)
- [Utilizza l'applicazione di tag per organizzare il tuo ambiente e per promuovere la responsabilità](#)
- [Strategie di applicazione di tag AWS](#)
- [Applicazione di tag alle risorse AWS](#)

Video correlati:

- [Next-generation permissions management \(Gestione delle autorizzazioni di ultima generazione\)](#)
- [Zero Trust: una prospettiva AWS](#)
- [Come posso utilizzare i limiti delle autorizzazioni per limitare utenti e ruoli e impedire l'escalation dei privilegi?](#)

Esempi correlati:

- [Laboratorio: limiti delle autorizzazioni IAM per delegare la creazione di ruoli](#)
- [Laboratorio: controllo degli accessi basato su tag IAM per EC2](#)

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 provider di identità centralizzato.

È necessario progettare processi per diverse modalità di guasto che possono causare un evento di emergenza. Ad esempio, in circostanze normali, gli utenti della tua forza lavoro si federano nel cloud utilizzando un provider di identità centralizzato ([SEC02-BP04](#)) per gestire i propri carichi di lavoro. Tuttavia, se il tuo provider di identità centralizzato genera un errore o la configurazione per la federazione nel cloud viene modificata, 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. Il processo di accesso di emergenza viene utilizzato 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. Considera quali guasti possono interessare ognuna di queste dipendenze e causare una situazione di emergenza. Puoi trovare le domande e le best practice nel [Principio di base dell'affidabilità](#), utile per identificare le modalità di errore e progettare sistemi più resilienti per 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 provider di identità primari e di standby e, se entrambi non sono disponibili, dichiarare un evento di emergenza per guasto del provider di identità.
- 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 descrivono

le circostanze in cui ogni processo deve essere o non deve essere utilizzato e indicano processi alternativi che possono essere applicati.

- I tuoi processi sono ben documentati con istruzioni e playbook dettagliati che possono essere seguiti 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 provider di identità 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 controllare i 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 avvisare in caso 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

Questa sezione fornisce indicazioni per la creazione di processi di accesso di emergenza per diverse modalità di errore relative ai carichi di lavoro distribuiti su AWS, a partire da linee guida comuni che si applicano 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 i prerequisiti e i 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 provider di identità 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 IAM users 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 preliminarmente le risorse, non si ha alcuna dipendenza dalle API del piano di controllo di AWS (utilizzate per creare e modificare risorse AWS), che potrebbero non essere disponibili in caso di emergenza. Inoltre, creando preliminarmente le risorse IAM, non è necessario tenere conto di [potenziali ritardi dovuti alla coerenza finale](#).
- Includi i processi di accesso di emergenza nei tuoi piani di gestione degli incidenti ([SEC10-BP02](#)). Documenta in che modo viene tenuta traccia degli eventi di emergenza e come essi 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 ogni 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 dei colleghi o dei manager dell'utente, a seconda dei casi. Il processo

di approvazione deve funzionare efficacemente sia all'interno che 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.

- Verifica che il processo generi log di controllo ed eventi dettagliati per i tentativi riusciti e falliti di ottenere l'accesso di emergenza. Monitora sia il processo di richiesta sia il meccanismo di accesso di emergenza per rilevare usi impropri o accessi non autorizzati. Metti in correlazione l'attività con gli eventi di emergenza in corso dal tuo sistema di gestione degli incidenti e avvisa quando le azioni si verificano al di fuori dei periodi di tempo previsti. Ad esempio, devi monitorare e inviare avvisi in merito ad attività nell'Account AWS di accesso di emergenza, poiché non dovrebbe mai essere utilizzato per le normali operazioni.
- 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 test di ripristino di emergenza ([REL13-BP03](#)).

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

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

Nell'improbabile eventualità che il provider di identità 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 caso critico, puoi fornire un processo di accesso di emergenza a 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 provider di identità centralizzati tornino online. Ad esempio, il tuo provider di identità 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 account di emergenza a un Account AWS creato preliminarmente, che viene utilizzato esclusivamente per questo tipo di accessi e dispone di risorse AWS (come ruoli IAM e IAM users) 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 di accesso di emergenza IAM 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:

- Creare preliminarmente un set di [IAM users](#) per gli amministratori di emergenza nell'account di accesso di emergenza con password complesse e token MFA associati. Questi IAM users 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 IAM user 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 IAM users con le relative password di lunga durata e i token MFA associati.
- È possibile utilizzare l'accesso di emergenza come [utente root dell'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 che esiste 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 il log eventi della tua vault aziendale per identificare quale amministratore ha utilizzato la password dell'utente root.

Modalità di errore 2: la configurazione del provider di identità su 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 IAM Identity Center con un provider di identità esterno o creare un provider di identità IAM ([SEC02-BP04](#)). In genere, la configurazione viene effettuata importando un documento XML di metadati SAML fornito dal provider di identità. Il documento XML di metadati include un certificato X.509 corrispondente a una chiave privata utilizzata dal provider di identità 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, costituendo una situazione di emergenza.

In un caso di emergenza di questo tipo, puoi fornire agli amministratori di 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 di identità e riattiva la federazione aggiornando la configurazione del provider di identità esterno e importando l'ultimo documento XML di metadati SAML rilasciato dal provider di identità. 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 descritti 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 di identità per accedere solo all'account amministratore di Centro di identità ed eseguire azioni sul Centro di identità in quell'account.

Modalità di errore 3: blocco del Centro di identità

Nell'improbabile eventualità di un blocco di IAM Identity Center o di una Regione AWS, ti consigliamo di eseguire una configurazione per fornire l'accesso temporaneo alla AWS Management Console.

Il processo di accesso di emergenza utilizza la federazione diretta rilasciata dal provider di identità a un ruolo IAM per accedere a un account di emergenza. Per informazioni dettagliate sulle

considerazioni relative al processo e alla progettazione, consulta [Configurare l'accesso di emergenza alla AWS Management Console](#).

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 users, e, in modo facoltativo, i provider di identità 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 utilizzare [AWS CloudFormation StackSets con AWS Organizations](#) per creare tali risorse negli account dei membri della tua organizzazione.
- Crea Policy di controllo dei servizi AWS Organizations ([SCP](#)) 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 ha 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 provider di identità utilizzato per la federazione dell'accesso ad AWS non è disponibile; per la Modalità di errore 2: la configurazione del provider di identità su AWS è stata modificata o è scaduta

- Crea preliminarmente le risorse in base al meccanismo scelto per l'accesso di emergenza:
 - Utilizza IAM users: crea preliminarmente IAM users con password complesse e dispositivi MFA associati.
 - Usa l'utente root dell'account di emergenza: configura l'utente root con una password sicura e archivia la password nel tuo archivio 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 di identità

- Come spiegato nei dettagli in [Configurare l'accesso di emergenza alla AWS Management Console](#), per l'accesso di emergenza a un Account AWS, crea un provider di identità IAM per abilitare la federazione SAML diretta dal tuo provider di identità.
- 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 provider di identità 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 AWS Management Console](#)
- [Abilitazione degli utenti federati SAML 2.0 per accedere a AWS Management Console](#)
- [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 customer playbook framework](#)
- [AWS incident response playbook samples](#)

SEC03-BP04 Riduzione delle autorizzazioni in modo continuo

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

Risultato desiderato: le policy di autorizzazione devono attenersi al 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 in cui le credenziali vengano inavvertitamente esposte o si acceda 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, le policy di autorizzazione permissiva possono essere utilizzate 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 costantemente 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 degli utenti e dei ruoli 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. [Controllo dell'accesso basato sugli attributi \(ABAC\)](#) può aiutare a semplificare la gestione delle autorizzazioni, in quanto è possibile fornire autorizzazioni agli utenti utilizzando i loro attributi invece di allegare le policy di autorizzazione direttamente a ciascun utente.

Passaggi dell'implementazione

- Utilizza [AWS Identity and Access Management Access Analyzer](#): IAM Access Analyzer aiuta a identificare le risorse nell'organizzazione e negli account, come ad esempio bucket Amazon Simple Storage Service (Amazon S3) o ruoli IAM che sono [condivisi con un'entità esterna](#).
- Utilizza la [generazione della policy IAM Access Analyzer](#): la generazione della policy IAM Access Analyzer aiuta a [creare policy di autorizzazione granulari basate su un utente IAM o su un'attività di accesso del ruolo](#).
- Stabilisci una tempistica accettabile e una policy di utilizzo per gli utenti e i ruoli IAM: utilizza il [timestamp dell'ultimo accesso](#) per [identificare gli utenti e i ruoli inutilizzati](#) e rimuoverli. Rivedi le informazioni sull'ultimo accesso al servizio e sull'ultima azione per identificare e [delimitare 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 AWS Management Console e consentono di incorporarle in modo programmatico nei flussi di lavoro dell'infrastruttura e negli strumenti automatizzati.
- Considera la [registrazione degli eventi di dati in AWS CloudTrail](#): per impostazione predefinita, CloudTrail non registra eventi di dati come le attività a livello di oggetto Amazon S3 (ad esempio, GetObject e DeleteObject) o le attività della tabella Amazon DynamoDB (ad esempio, PutItem e DeleteItem). Considera la possibilità di abilitare la registrazione di questi eventi per stabilire quali utenti e ruoli devono accedere a specifici oggetti Amazon S3 o elementi di tabelle DynamoDB.

Risorse

Documenti correlati:

- [Assegnare il privilegio minimo](#)
- [Rimozione di credenziali non necessarie](#)
- [Cosa è AWS CloudTrail?](#)
- [Working with Policies](#) (Gestire le policy)
- [Registrazione e monitoraggio in DynamoDB](#)

- [Abilitazione della registrazione di eventi CloudTrail per bucket e oggetti Amazon S3](#)
- [Recupero dei report delle credenziali per l'Account AWS](#)

Video correlati:

- [Become an IAM Policy Master in 60 Minutes or Less](#) (Diventa un IAM Policy Master in 60 minuti)
- [Separation of Duties, Least Privilege, Delegation, and CI/CD](#) (Separazione dei compiti, privilegio minimo, delega e integrazione e distribuzione continua (CI/CD))
- [AWS re:Inforce 2022 - AWS Identity and Access Management \(IAM\) deep dive](#) [AWS re:Inforce 2022 - Approfondimento su AWS Identity and Access Management (IAM)]

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

Stabilisci controlli comuni che limitano l'accesso a tutte le identità nella tua organizzazione. Ad esempio, puoi limitare l'accesso a Regioni AWS specifiche o impedire agli operatori di eliminare risorse comuni, come ad esempio un ruolo IAM utilizzato per il team di sicurezza centrale.

Anti-pattern comuni:

- Esecuzione di carichi di lavoro nell'account di amministratore dell'organizzazione.
- Esecuzione di carichi di lavoro di produzione e non di produzione nello stesso account.

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

Guida all'implementazione

Man mano che aumenti e gestisci carichi di lavoro aggiuntivi in AWS, devi separarli utilizzando gli account e gestire questi ultimi utilizzando AWS Organizations. Ti consigliamo di stabilire limiti di autorizzazione comuni che limitano l'accesso a tutte le identità nella tua organizzazione. Ad esempio, puoi limitare l'accesso a Regioni AWS specifiche o impedire al tuo team di eliminare risorse comuni, come ad esempio un ruolo IAM utilizzato dal team di sicurezza centrale.

Puoi iniziare implementando delle policy di controllo dei servizi di esempio, come una policy che impedisce agli utenti di disabilitare i servizi chiave. Le policy di controllo dei servizi utilizzano il linguaggio di policy IAM e consentono di stabilire i controlli a cui aderiscono tutti i principali IAM

(utenti e ruoli). Puoi limitare l'accesso a specifiche azioni del servizio, risorse e in base a condizioni specifiche per soddisfare le esigenze di controllo degli accessi della tua organizzazione. Se necessario, puoi definire eccezioni ai limiti definiti. Ad esempio, puoi limitare le azioni del servizio per tutte le entità IAM nell'account tranne per un ruolo amministratore specifico.

Ti consigliamo di evitare di eseguire carichi di lavoro nell'account di gestione. L'account di gestione deve essere utilizzato per governare e distribuire i guardrail di sicurezza che influiscono sugli account membri. Alcuni servizi AWS supportano l'uso di un account amministratore delegato. Se è disponibile, devi utilizzare questo account delegato anziché l'account di gestione. È necessario limitare scrupolosamente l'accesso all'account dell'amministratore dell'organizzazione.

L'utilizzo di una strategia multi-account ti consente di avere una maggiore flessibilità nell'applicazione di guardrail ai tuoi carichi di lavoro. L'architettura di riferimento per la sicurezza AWS fornisce le indicazioni prescrittive su come progettare la struttura del tuo account. I servizi AWS come AWS Control Tower forniscono le funzionalità per gestire centralmente i controlli preventivi e investigativi all'interno dell'organizzazione. Definisci uno scopo chiaro per ogni account o unità organizzativa all'interno della tua organizzazione e limita i controlli in linea con tale scopo.

Risorse

Documenti correlati:

- [AWS Organizations](#)
- [Policy di controllo dei servizi \(Service Control Policies, SCP\)](#)
- [Get more out of service control policies in a multi-account environment \(Ottieni di più dalle policy di controllo dei servizi in un ambiente multi-account\)](#)
- [AWS Security Reference Architecture \(AWS SRA\) \(Architettura di riferimento per la sicurezza AWS \(AWS SRA\)\)](#)

Video correlati:

- [Enforce Preventive Guardrails using Service Control Policies \(Applicazione di guardrail preventivi utilizzando le policy di controllo dei servizi\)](#)
- [Building governance at scale with AWS Control Tower \(Creazione di una governance su vasta scala con AWS Control Tower\)](#)
- [AWS Identity and Access Management deep dive \(Approfondimenti su AWS Identity and Access Management\)](#)

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

Integra i controlli degli accessi con il ciclo di vita degli operatori e delle applicazioni e con il tuo provider di federazione centralizzata. Ad esempio, rimuovi l'accesso di un utente quando lascia l'organizzazione o cambia ruolo.

Quando gestisci i carichi di lavoro utilizzando account separati, in alcuni casi sarà necessario condividere le risorse tra tali account. Ti consigliamo di condividere le risorse utilizzando [AWS Resource Access Manager \(AWS RAM\)](#). Questo servizio ti consente di condividere in modo semplice e sicuro le risorse AWS all'interno della tua organizzazione AWS Organizations e delle unità organizzative. Con AWS RAM, l'accesso alle risorse condivise viene automaticamente concesso o revocato quando gli account vengono spostati da e verso l'organizzazione o l'unità organizzativa con cui sono condivisi. In questo modo puoi garantire che le risorse vengano condivise solo con gli account desiderati.

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

Guida all'implementazione

Ciclo di vita degli accessi utente: implementa una policy per il ciclo di vita degli accessi utente per i nuovi entranti, le modifiche alle funzioni lavorative e gli uscenti per garantire l'accesso solo agli utenti attuali.

Risorse

Documenti correlati:

- [Controllo dell'accesso basato su attributi \(Attribute-Based Access Control, ABAC\)](#)
- [Assegnare il privilegio minimo](#)
- [IAM Access Analyzer](#)
- [Rimozione di credenziali non necessarie](#)
- [Lavorare con le policy](#)

Video correlati:

- [Become an IAM Policy Master in 60 Minutes or Less \(Diventa un IAM Policy Master in 60 minuti\)](#)
- [Separation of Duties, Least Privilege, Delegation, and CI/CD \(Separazione dei compiti, privilegio minimo, delega e integrazione e distribuzione continua \(CI/CD\)\)](#)

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

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

Risultato desiderato: sapere quali risorse AWS sono condivise e con chi. Monitora e sottoponi costantemente a 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 collegate a risorse, ad esempio [policy di bucket Amazon Simple Storage Service \(Amazon S3\)](#) o consentendo a un principale in 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 la [sicurezza comprovabile](#) per identificare tutti i percorsi di accesso a una risorsa dall'esterno del suo account. Esamina continuamente le policy delle risorse e segnala i risultati dell'accesso pubblico e multi-account per semplificare l'analisi di accessi potenzialmente estesi. Considera di configurare IAM Access Analyzer con AWS Organizations per assicurarti di avere visibilità su tutti gli account. IAM Access Analyzer consente inoltre di [vedere in anteprima i risultati](#) prima di implementare le autorizzazioni della risorsa. Questo consente di convalidare che le modifiche alla policy concedono solo l'accesso multi-account e pubblico autorizzati alle risorse. Quando progetti l'accesso multi-account, puoi utilizzare le [policy di attendibilità](#) per controllare in quali casi un ruolo può essere assunto. Ad esempio, puoi utilizzare la chiave di condizione [PrincipalOrgId per respingere il tentativo di assumere un ruolo al di fuori di AWS Organizations](#).

[AWS Config può segnalare le risorse](#) che non sono configurate correttamente e, attraverso i controlli delle policy AWS Config, può rilevare le risorse con accesso pubblico configurato. Servizi quali [AWS Control Tower](#) e [AWS Security Hub](#) semplificano l'implementazione dei controlli e guardrail investigativi su AWS Organizations per identificare e correggere le risorse esposte pubblicamente. Ad esempio, AWS Control Tower ha un guardrail gestito in grado di rilevare l'eventuale presenza di [snapshot Amazon EBS ripristinabili da Account AWS](#).

Passaggi dell'implementazione

- Considera di abilitare [AWS Config per AWS Organizations](#): AWS Config consente di aggregare i risultati di più account all'interno di un AWS Organizations a un account amministratore delegato. In questo modo si ottiene una visione completa che consente di [implementare Regole di AWS Config su più account per rilevare le risorse accessibili pubblicamente](#).
- Configura AWS Identity and Access Management Access Analyzer. IAM Access Analyzer ti aiuta a identificare le risorse nell'organizzazione e negli account, come ad esempio bucket Amazon S3 o ruoli IAM che sono [condivisi con un'entità esterna](#).
- Utilizza la riparazione automatica in AWS Config per rispondere alle modifiche della configurazione di accesso pubblico dei bucket Amazon S3: [puoi riattivare automaticamente le impostazioni di blocco dell'accesso pubblico per i bucket Amazon S3](#).
- Implementa il monitoraggio e gli avvisi per stabilire se i bucket Amazon S3 sono diventati pubblici: devi disporre di [monitoraggio e avvisi](#) per stabilire quando Amazon S3 Block Public Access è disabilitato e se i bucket Amazon S3 diventano pubblici. Inoltre, se stai utilizzando AWS Organizations, puoi creare una [policy di controllo del servizio](#) che impedisce di modificare le policy Amazon S3 di accesso pubblico. AWS Trusted Advisor controlla i bucket Amazon S3 che hanno 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](#) (Come utilizzare AWS Config per monitorare e gestire i bucket Amazon S3 che consentono l'accesso pubblico). Durante la revisione degli accessi, è importante considerare quali tipi di dati sono contenuti nei bucket Amazon S3. [Amazon Macie](#) aiuta a scoprire e a proteggere i dati sensibili, come PII, PHI, e le credenziali, come le chiavi private o quelle AWS.

Risorse

Documenti correlati:

- [Utilizzo di AWS Identity and Access Management Access Analyzer](#)
- [AWS Control Tower controls library](#) (Libreria di controlli di AWS Control Tower)
- [AWS Foundational Security Best Practices standard](#) (Standard AWS Foundational Security Best Practices)
- [AWS Config Managed Rules](#) (Regole gestite di AWS Config)
- [Riferimento dei controlli AWS Trusted Advisor](#)
- [Monitoraggio dei risultati dei controlli AWS Trusted Advisor con Amazon EventBridge](#)
- [Managing AWS Config Rules Across All Accounts in Your Organization](#) (Gestire le regole di configurazione AWS tra tutti gli account dell'organizzazione)
- [AWS Config e AWS Organizations](#)

Video correlati:

- [Best Practices for securing your multi-account environment \(Best practice per la protezione dell'ambiente multi-account\)](#)
- [Dive Deep into IAM Access Analyzer](#) (Approfondire l'analisi degli accessi IAM)

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 ambiente, come ad esempio ambienti di sviluppo, di test e di produzione. Tuttavia, la presenza di costrutti di separazione non limita la possibilità di condividere in modo sicuro. La condivisione di componenti che si sovrappongono 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 indesiderati utilizzando metodi sicuri per condividere le risorse all'interno dell'organizzazione e contribuire all'iniziativa di prevenzione della perdita di 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. I tempi di risoluzione in caso di guasti multipli sono ridotti e la sicurezza nel determinare quando un componente non è più necessario è aumentata. Per una guida prescrittiva sull'analisi delle risorse condivise dall'esterno, consulta [SEC03-BP07 Analisi dell'accesso pubblico e multi-account](#).

Anti-pattern comuni:

- Mancanza di un processo per il monitoraggio continuo e segnalazione automatica di azioni 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 i controlli e i modelli di accesso per gestire il consumo di risorse condivise in modo sicuro e solo con entità fidate. Monitora le risorse condivise e controllane costantemente l'accesso ricevendo un avviso in caso di condivisione inappropriata o inaspettata. Consulta [Analisi dell'accesso pubblico e multi-account](#) come supporto per stabilire una governance che riduca l'accesso esterno alle sole risorse che lo richiedono e per definire un processo di monitoraggio continuo e di avviso automatico.

La condivisione multi-account in AWS Organizations è supportata da [una serie di servizi AWS](#), come [AWS Security Hub](#), [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 può trasferire i risultati dai singoli account a un account centrale in cui è possibile visualizzare tutti i risultati. AWS Backup può eseguire un backup di una risorsa e condividerlo tra gli account. Puoi utilizzare [AWS Resource Access Manager](#) (AWS RAM) per condividere altre risorse comuni, quali [sottoreti VPC e allegati Transit Gateway](#), [AWS Network Firewall](#) o [pipeline Amazon SageMaker](#).

Per limitare l'account alla condivisione di risorse solo all'interno dell'organizzazione, utilizza le [policy di controllo dei servizi](#) (Service Control Policies, SCP) per impedire l'accesso ai principali esterni. Quando condividi le risorse, combina controlli basati sull'identità e controlli di rete per [creare un perimetro di dati per l'organizzazione](#) in modo da proteggere dall'accesso non intenzionale. 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

che possono essere condivise e impediscono la condivisione o l'esposizione di risorse che non sono consentite. Ad esempio, nell'ambito del perimetro dei dati, è possibile utilizzare le policy degli endpoint VPC e la condizione `AWS:PrincipalOrgId` per assicurarsi che le identità che accedono ai bucket Amazon S3 appartengano alla propria organizzazione. È importante notare che le [policy di controllo dei servizi non si applicano ai ruoli correlati ai servizi \(Service-Linked Roles, LSR\) o ai principali del servizio AWS](#).

Quando utilizzi Amazon S3, [disabilita le ACL per il bucket Amazon S3](#) e utilizza le policy IAM per definire il controllo degli accessi. Per [delimitare un accesso a un'origine Amazon S3](#) da [Amazon CloudFront](#), migra dall'identità di accesso origine (OAI) al controllo di accesso origine (OAC) che supporta funzionalità aggiuntive, inclusa 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 terzi l'accesso alle risorse stesse. Per una guida prescrittiva sulla gestione delle autorizzazioni per la condivisione di risorse all'esterno, 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 creata e gestita centralmente. 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 Organizations.

2. Integrazione delle AWS Organizations con i servizi AWS.

Quando si abilita un servizio AWS a svolgere attività per conto dell'utente negli account membri dell'organizzazione, AWS Organizations crea un ruolo IAM collegato al servizio in ogni account membro. L'accesso attendibile deve essere gestito tramite la AWS Management Console, le API AWS o la AWS CLI. Per una guida prescrittiva sull'abilitazione dell'accesso attendibile, consulta [Uso di AWS Organizations con altri servizi AWS](#) e [Servizi AWS che puoi utilizzare con Organizations](#).

3. Definizione di un perimetro di dati.

Il perimetro AWS è tipicamente rappresentato come un'organizzazione gestita da AWS Organizations. Insieme alle reti e ai sistemi on-premise, l'accesso alle risorse AWS è ciò che

molti considerano il perimetro di My AWS. L'obiettivo del perimetro è verificare che l'accesso sia consentito se l'identità è attendibile, la risorsa è attendibile e la rete è conforme.

a. Definizione e implementazione dei perimetri.

Segui i passaggi descritti in [Perimeter implementation](#) (Implementazione del perimetro) nel whitepaper Building a Perimeter on AWS (Costruire un perimetro su AWS) per qualsiasi condizione di autorizzazione. Per una guida prescrittiva sulla protezione del livello di rete, consulta [Protezione delle reti](#).

b. Monitoraggio e segnalazione continui.

[AWS Identity and Access Management Access Analyzer](#) aiuta a identificare le risorse dell'organizzazione e gli account condivisi con entità esterne. Puoi integrare [IAM Access Analyzer con AWS Security Hub](#) per inviare e aggregare i risultati di una risorsa da IAM Access Analyzer a Security Hub per analizzare la sicurezza dell'ambiente. Per abilitare l'integrazione, abilita sia IAM Access Analyzer che Security Hub in ogni Regione per ogni account. Puoi anche utilizzare Regole di AWS Config per eseguire l'audit della configurazione e avvisare la parte interessata mediante [AWS Chatbot con AWS Security Hub](#). Puoi quindi utilizzare i [Documenti di AWS Systems Manager](#) per adottare i provvedimenti correttivi alle risorse non conformi.

c. Per una guida prescrittiva sul monitoraggio e sull'avviso continuo delle risorse condivise esternamente, consulta [Analisi dell'accesso pubblico e multi-account](#).

4. Utilizza la condivisione delle risorse nei servizi AWS e delimitale di conseguenza.

Molti servizi AWS consentono di condividere le risorse con un altro account o di puntare a una risorsa di un altro account, come [Amazon Machine Image \(AMI\)](#) e [AWS Resource Access Manager \(AWS RAM\)](#). Delimita l'API `ModifyImageAttribute` per specificare gli account affidabili con cui condividere l'AMI. Specifica la condizione `ram:RequestedAllowsExternalPrincipals` quando si utilizza AWS RAM per limitare la condivisione solo alla propria organizzazione, per evitare l'accesso da parte di identità non affidabili. Per indicazioni e considerazioni prescrittive [Resource sharing and external targets](#) (Condivisione delle risorse e target esterni).

5. Utilizzare AWS RAM per condivisioni sicure con un account o con altri Account AWS.

[AWS RAM](#) consente di condividere in modo sicuro le risorse create con i ruoli e gli utenti del proprio account e con altri utenti 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 verificabilità

grazie alle integrazioni con Amazon CloudWatch e AWS CloudTrail, che non si ottengono quando si utilizza l'accesso multi-account.

Se si dispone di risorse condivise in precedenza utilizzando una policy basata sulle risorse, è possibile utilizzare l'API [PromoteResourceShareCreatedFromPolicy](#) o un'API equivalente per promuovere il passaggio da una condivisione di risorse a una condivisione completa di risorse AWS RAM.

In alcuni casi, potrebbe essere necessario adottare ulteriori misure per condividere le risorse. Ad esempio, per condividere un'istanza crittografata è necessario [condividere una chiave AWS KMS](#).

Risorse

Best practice correlate:

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

Documenti correlati:

- [Il proprietario del bucket concede autorizzazioni multi-account per gli oggetti che non sono di sua proprietà](#)
- [How to use Trust Policies with IAM](#) (Come utilizzare le policy di attendibilità con IAM)
- [Building Data Perimeter on AWS](#) (Creazione del perimetro dei dati in AWS)
- [How to use an external ID when granting a third party access to your AWS resources](#) (Come utilizzare un ID esterno quando si concede a una terza parte l'accesso alle risorse AWS)
- [Servizi AWS che puoi utilizzare con AWS Organizations](#)
- [Establishing a data perimeter on AWS: Allow only trusted identities to access company data](#) (Applicazione di un perimetro dei dati in AWS: consentire l'accesso ai dati aziendali solo alle identità attendibili)

Video correlati:

- [Granular Access with AWS Resource Access Manager](#) (Accesso granulare con Gestione degli accessi alle risorse AWS)
- [Securing your data perimeter with VPC endpoints](#) (Protezione del perimetro dei dati con gli endpoint VPC)
- [Establishing a data perimeter on AWS](#) (Applicazione di un perimetro dei dati in AWS)

Strumenti correlati:

- [Esempi di policy sul perimetro dei 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 terzi la gestione di una parte dei dati. La gestione dei permessi per il sistema gestito da terzi 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 congiuntamente la portata dell'impatto e il rischio di accesso non intenzionale.

Risultato desiderato: le credenziali AWS Identity and Access Management (IAM) a lungo termine, le chiavi di accesso IAM e le chiavi segrete associate a un utente possono essere utilizzate da chiunque, purché le credenziali siano valide e attive. L'utilizzo di credenziali temporanee e di un ruolo IAM consente di migliorare la sicurezza generale riducendo l'impegno per la manutenzione delle credenziali a lungo termine, compresi i costi di gestione e di funzionamento di questi dati sensibili. Utilizzando un identificatore univoco universale (UUID) per l'ID esterno nella policy di attendibilità IAM e mantenendo sotto il proprio controllo le policy IAM collegate al ruolo IAM, puoi sottoporre a audit e verificare che l'accesso concesso a terzi non sia troppo permissivo. Per una guida prescrittiva sull'analisi delle risorse condivise dall'esterno, consulta [SEC03-BP07 Analisi dell'accesso pubblico e multi-account](#).

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 terzi 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, devi definire una policy di attendibilità utilizzando la [condizione di 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 gestire ruoli IAM per le applicazioni esterne ad AWS che utilizzano le 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. Ad esempio, AWS Well-Architected Tool consente la [condivisione di un carico di lavoro](#) con altri Account AWS e [AWS Resource Access Manager](#) ti aiuta a condividere in modo sicuro una risorsa AWS di tua proprietà con altri account.

Passaggi dell'implementazione

1. Utilizzare i 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 da terze parti per l'assistenza ai propri clienti. I ruoli multi-account consentono di concedere l'accesso alle risorse AWS del proprio account in modo sicuro a terzi, come i AWS Partner 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 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. Utilizzare un ID esterno con terze parti.

L'utilizzo di un [ID esterno](#) consente di designare chi può assumere un ruolo in una policy di attendibilità IAM. La policy di attendibilità può richiedere che l'utente che assume il ruolo dichiari la condizione e l'obiettivo in cui sta operando. Inoltre, il proprietario dell'account può consentire l'assunzione del ruolo solo in determinate circostanze. La funzione principale dell'ID esterno è quella di affrontare e prevenire il problema del [confused deputy](#).

Utilizza un ID esterno se sei il proprietario di un Account AWS e hai configurato un ruolo per una terza parte che accede ad altri Account AWS oltre al tuo, oppure quando ti trovi nella posizione di assumere ruoli per conto di diversi clienti. Collabora con la terza parte o con il AWS Partner per stabilire una condizione di ID esterno da includere nelle policy di attendibilità IAM.

3. Utilizzare ID esterni universalmente univoci.

Implementa un processo che generi un valore univoco casuale per un ID esterno, ad esempio un identificatore univoco universale (UUID). Una terza parte che riutilizza gli ID esterni tra diversi clienti non risolve il problema del confused deputy, perché il cliente A potrebbe essere in grado di visualizzare i dati del cliente B utilizzando l'ARN del ruolo del cliente B insieme all'ID esterno duplicato. In un ambiente multi-tenant, in cui una terza parte supporta più clienti con diversi Account AWS, la terza parte deve utilizzare un ID univoco diverso come ID esterno per ogni Account AWS. La terza parte è responsabile del rilevamento di ID esterni duplicati e della mappatura sicura di ciascun cliente al rispettivo ID esterno. La terza parte deve verificare di poter assumere il ruolo solo quando specifica l'ID esterno. La terza parte deve astenersi dal memorizzare l'ARN del ruolo del cliente e l'ID esterno fino a quando non è richiesto l'ID esterno.

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 di 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'unicità e i formati in modo coerente tra i clienti.

4. Rendere 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 dettagli sulla gestione delle chiavi, consulta [Identity Management](#) (Gestione dell'identità). Collaborare inoltre con il team dell'Account AWS e con la terza parte

per stabilire un runbook di mitigazione dei rischi. Per una guida prescrittiva sulla risposta e la mitigazione dell'impatto potenziale di un incidente di sicurezza, consulta [Incident response](#) (Risposta agli incidenti).

5. Verifica che l'impostazione abbia una guida prescrittiva o sia automatizzata.

La policy creata per l'accesso multi-account deve seguire il [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 una traccia verificabile. Per ulteriori informazioni sull'utilizzo di un modello AWS CloudFormation per creare ruoli trasversali agli account, consulta [Cross-Account Roles](#) (Ruoli multi-account).

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 derive come parte della pratica di audit.

6. Account per le 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 i cambiamenti e i fallimenti e 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 a audit l'uso del ruolo e del datastore degli ID esterni. Devi essere pronto a revocare l'accesso a terzi, 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 una guida prescrittiva sui metodi di rilevamento, consulta [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 pubblico e multi-account](#)

- [SEC04 Rilevamento](#)

Documenti correlati:

- [Il proprietario del bucket concede autorizzazioni multi-account per gli oggetti che non sono di sua proprietà](#)
- [How to use trust policies with IAM roles](#) (Come utilizzare le policy di attendibilità con i ruoli IAM)
- [Delega dell'accesso tra Account AWS tramite i ruoli IAM](#)
- [How do I access resources in another Account AWS using IAM?](#) (Come faccio ad accedere alle risorse di un altro account AWS utilizzando IAM?)
- [Best practice per la sicurezza in IAM](#)
- [Logica di valutazione della policy multiaccount](#)
- [Come utilizzare un ID esterno quando si concede a una terza parte l'accesso alle proprie risorse AWS](#)
- [Collecting Information from AWS CloudFormation Resources Created in External Accounts with Custom Resources](#) (Raccolta di informazioni dalle risorse AWS CloudFormation create in account esterni con risorse personalizzate)
- [Securely Using External ID for Accessing AWS Accounts Owned by Others](#) (Utilizzo sicuro dell'ID esterno per l'accesso agli account AWS di proprietà di altri)
- [Extend IAM roles to workloads outside of IAM with IAM Roles Anywhere](#) (Estendere i ruoli IAM a carichi di lavoro esterni a IAM con IAM Roles Anywhere)

Video correlati:

- [How do I allow users or roles in a separate Account AWS access to my Account AWS?](#) (Come posso consentire agli utenti o ai ruoli di un account AWS separato di accedere al mio account AWS?)
- [AWS re:Invent 2018: Become an IAM Policy Master in 60 Minutes or Less](#) (Diventa un IAM Policy Master in 60 minuti)
- [AWS Knowledge Center Live: IAM Best Practices and Design Decisions](#) (Knowledge Center AWS in diretta: best practice e decisioni di progettazione IAM)

Esempi correlati:

- [Well-Architected Lab - Lambda cross account IAM role assumption \(Level 300\)](#) [Well-Architected Lab: Assunzione di ruoli IAM per account incrociati Lambda (livello 300)]
- [Configure cross-account access to Amazon DynamoDB](#) (Configurare l'accesso multi-account ad Amazon DynamoDB)
- [AWS STS Network Query Tool](#) (Strumento di consultazione della 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 l'infrastruttura come codice (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 distribuisce 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 una distribuzione 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 registri di servizi e applicazioni](#)

- [SEC04-BP02 Analisi di log, risultati e parametri a livello centrale](#)
- [SEC04-BP03 Automazione delle risposte agli eventi](#)
- [SEC04-BP04 Implementazione di eventi di sicurezza fruibili](#)

SEC04-BP01 Configurazione dei registri 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 dei servizi e delle applicazioni AWS in modo tempestivo, quando è necessario soddisfare un processo o un obbligo interno, come la risposta a un incidente di sicurezza. Considera la possibilità di centralizzare i log per ottenere migliori risultati operativi.

Anti-pattern comuni:

- Log archiviati in modo perpetuo o cancellati troppo presto.
- Tutti possono accedere ai log.
- Affidarsi interamente 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 della definizione di questa best practice: implementare un meccanismo di root cause analysis (RCA) per gli incidenti di sicurezza e una fonte di prove per gli obblighi 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 che sono avvenute determinate

azioni di interesse. È fondamentale selezionare, attivare, memorizzare e impostare i meccanismi di interrogazione e recupero e gli avvisi.

Passaggi dell'implementazione

- Selezionare e abilitare le origini dei log. Prima di un'indagine di sicurezza, devi acquisire i log rilevanti per ricostruire retroattivamente l'attività in un Account AWS. Seleziona e attiva le origini dei log rilevanti per i carichi di lavoro.

I criteri di selezione delle origini dei log devono essere basati 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 esso un bucket Amazon S3.

AWS CloudTrail è un servizio di registrazione che tiene traccia delle chiamate API effettuate su un Account AWS, catturando l'attività del servizio AWS. È abilitato per impostazione predefinita e prevede una conservazione di 90 giorni degli eventi di gestione che possono essere [recuperati attraverso la cronologia degli eventi CloudTrail](#) utilizzando la AWS Management Console, la AWS CLI o un AWS SDK. Per una conservazione e una visibilità più lunghe degli eventi di 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 mantiene 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 un VPC di abilitare i log del traffico di rete e del DNS utilizzando rispettivamente i [log di flusso VPC](#) e i [log delle query del resolver Amazon Route 53](#) e di inviarli in streaming a un bucket Amazon S3 o a 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 resolver 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), pronti per essere interrogati. 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 di AWS Config, risultati 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 registrazione e monitoraggio, consulta [Appendix A: Cloud capability definitions – Logging and Events](#) (Appendice A: Definizioni

delle capacità del cloud - Registrazione ed eventi) della [AWS Security Incident Response Guide](#) (Guida alla risposta agli incidenti di sicurezza di AWS).

- Ricercare le funzionalità di log per ogni servizio e applicazione AWS: ogni servizio e applicazione AWS offre opzioni per l'archiviazione dei log, ognuna con capacità di conservazione e ciclo di vita proprie. I due servizi di archiviazione dei 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 economicità e per la flessibilità del ciclo di vita. Se l'opzione principale di registrazione è Amazon CloudWatch Logs, puoi prendere in considerazione l'archiviazione dei log ad accesso meno frequente su Amazon S3.
- Selezionare l'archiviazione dei log: la scelta dell'archiviazione dei log è generalmente legata allo strumento di query utilizzato, alle capacità di conservazione, alla familiarità e al costo. Le opzioni principali per l'archiviazione dei log sono un bucket Amazon S3 o un gruppo CloudWatch Log.

Un bucket Amazon S3 offre la possibilità di un'archiviazione economica e duratura, con una policy opzionale per il ciclo di vita. I log archiviati nei bucket Amazon S3 possono essere interrogati utilizzando servizi come Amazon Athena.

Un gruppo di log di CloudWatch offre un'archiviazione durevole e una funzione di interrogazione integrata attraverso CloudWatch Logs Insights.

- Identificare la conservazione appropriata dei log: quando utilizzi un bucket Amazon S3 o un gruppo di log CloudWatch per archiviare i log, è necessario stabilire cicli di vita adeguati per ogni origine di log per 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 della disponibilità e della conservazione deve essere in linea con i requisiti di sicurezza e con un insieme di mandati statutari, normativi e aziendali.
- Abilitare la registrazione per ogni servizio e applicazione AWS con policy di conservazione e ciclo di vita adeguate: per ogni servizio o applicazione AWS nell'organizzazione, cerca le indicazioni specifiche per la configurazione della registrazione:
 - [Configure AWS CloudTrail Trail](#) (Configurazione di un percorso AWS CloudTrail)
 - [Configure VPC Flow Logs](#) (Configurazione di VPC Flow Logs)
 - [Configure Amazon GuardDuty Finding Export](#) (Configurazione dell'esportazione di risultati Amazon GuardDuty)
 - [Configure AWS Config recording](#) (Configurazione della registrazione di AWS Config)
 - [Configure AWS WAF web ACL traffic](#) (Configurazione del traffico ACL web di AWS WAF)

- [Configure AWS Network Firewall network traffic logs](#) (Configurazione dei log del traffico di rete del firewall di rete AWS)
- [Configure Elastic Load Balancing access logs](#) (Configurazione dei log di accesso di Elastic Load Balancing)
- [Configure Amazon Route 53 resolver query logs](#) (Configurazione dei log delle query del resolver di Amazon Route 53)
- [Configure Amazon RDS logs](#) (Configurazione dei log di Amazon RDS)
- [Configure Amazon EKS Control Plane logs](#) (Configurazione dei log del piano di controllo di Amazon EKS)
- [Configure Amazon CloudWatch agent for Amazon EC2 instances and on-premises servers](#) (Configurazione dell'agente Amazon CloudWatch per istanze Amazon EC2 e server on-premise)
- Selezionare e implementare i meccanismi di interrogazione dei log: per le query sui log, puoi utilizzare [CloudWatch Logs Insights](#) per i dati archiviati nei gruppi di log di CloudWatch e [Amazon Athena](#) e [Amazon OpenSearch Service](#) per i dati archiviati in Amazon S3. Inoltre, puoi utilizzare strumenti di interrogazione di terze parti, come un servizio di gestione delle informazioni e degli eventi di sicurezza (SIEM).

Il processo di selezione di uno strumento di interrogazione 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 e che sia accessibile e manutenibile a lungo termine. Tieni presente che gli strumenti di interrogazione 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 interrogazione 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 massimizzare l'efficienza operativa, soprattutto durante le indagini su un evento di sicurezza.

- Utilizzare i log per gli avvisi: AWS fornisce avvisi attraverso diversi servizi di sicurezza:
 - [AWS Config](#) monitora e registra le configurazioni delle risorse AWS e consente di automatizzare la valutazione e la correzione delle configurazioni desiderate.
 - [Amazon GuardDuty](#) è un servizio di rilevamento delle minacce che monitora costantemente la presenza di attività dannose e di comportamenti non autorizzati per proteggere gli Account

AWS e i carichi di lavoro. GuardDuty acquisisce, aggrega e analizza le informazioni provenienti da origini, come ad esempio gestione AWS CloudTrail ed eventi di dati, log DNS, log di flusso VPC e log di audit Amazon EKS. GuardDuty estrae flussi di dati indipendenti direttamente da CloudTrail, log di flusso VPC, log di query DNS ed 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 registri a fini investigativi e di conformità.

- [AWS Security Hub](#) offre un unico luogo che aggrega, organizza e definisce le priorità degli avvisi di sicurezza o delle scoperte provenienti da più servizi AWS e da prodotti opzionali di terze parti, per fornire una visione 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 [Detection \(Rilevamento\) nella AWS Security Incident Response Guide](#) (Guida alla risposta agli incidenti di sicurezza di AWS).

Risorse

Best practice correlate:

- [SEC04-BP02 Analisi di log, risultati e parametri a livello centrale](#)
- [SEC07-BP04 Definizione della gestione del ciclo di vita dei dati](#)
- [SEC10-BP06 Distribuzione anticipata degli strumenti](#)

Documenti correlati:

- [AWS Security Incident Response Guide](#)
- [Nozioni di base su Amazon Security Lake](#)
- [Nozioni di base su: Amazon CloudWatch Logs](#)
- [Soluzione dei partner per la sicurezza: registrazione e monitoraggio](#)

Video correlati:

- [AWS re:Invent 2022 - Introducing Amazon Security Lake](#) (re:Invent 2022 - Introduzione ad Amazon Security Lake)

Esempi correlati:

- [Assisted Log Enabler for AWS](#) (Abilitatore di log assistito per AWS)
- [AWS Security Hub Findings Historical Export](#) (Esportazione cronologica dei risultati di AWS Security Hub)

Strumenti correlati:

- [Snowflake for Cybersecurity](#)

SEC04-BP02 Analisi di log, risultati e parametri a livello centrale

I team delle operazioni di sicurezza confidano nella raccolta di log e nell'utilizzo di strumenti di ricerca per scoprire potenziali eventi di interesse, che potrebbero indicare attività non autorizzate o modifiche involontarie. Tuttavia, la semplice analisi dei dati raccolti e l'elaborazione manuale delle informazioni non sono sufficienti per tenere il passo con il volume di informazioni provenienti da architetture complesse. Le sole analisi e i soli resoconti non facilitano l'assegnazione delle risorse giuste per lavorare a un evento in modo adeguato e nei tempi giusti.

Una best practice per creare un team per le operazioni di sicurezza preparato è integrare profondamente il flusso degli eventi di sicurezza e le scoperte in un sistema di notifica e flusso di lavoro, come un sistema di ticketing, un sistema di bug o altri sistemi riguardanti le informazioni di sicurezza o la gestione degli eventi (SIEM). Ciò elimina il flusso di lavoro da e-mail e report statici e consente di instradare, inoltrare e gestire eventi o risultati. Molte organizzazioni integrano anche gli avvisi di sicurezza nelle loro piattaforme di chat, collaborazione e di produttività per sviluppatori. Per le aziende che intraprendono la strada dell'automazione, un sistema di ticketing basato su API a bassa latenza offre una notevole flessibilità quando si pianifica "cosa automatizzare prima".

Questa best practice si applica non solo agli eventi di sicurezza generati dai messaggi di log che illustrano l'attività degli utenti o gli eventi di rete, ma anche a quelli generati dalle modifiche rilevate nell'infrastruttura stessa. La possibilità di rilevare le modifiche, determinare se una modifica è appropriata e quindi instradare tali informazioni al flusso di lavoro di correzione adatto è essenziale per mantenere e convalidare un'architettura sicura, in un contesto di modifiche difficili da individuare come indesiderabili per impedirne l'esecuzione tramite una combinazione di configurazioni AWS Identity and Access Management (IAM) e AWS Organizations.

Amazon GuardDuty e AWS Security Hub forniscono meccanismi di aggregazione, deduplicazione e analisi per i record di log che vengono resi disponibili anche tramite altri servizi AWS. GuardDuty

acquisisce, aggrega e analizza le informazioni da origini come AWS CloudTrail management and data events, log di VPC DNS e log di flusso VPC. Security Hub può acquisire, aggregare e analizzare output di GuardDuty, AWS Config, Amazon Inspector, Amazon Macie, AWS Firewall Manager e un numero significativo di prodotti di sicurezza di terze parti disponibili in Marketplace AWS, nonché il codice proprietario, se è stato compilato in modo adeguato. Sia GuardDuty sia Security Hub hanno un modello membro-amministratore che può aggregare risultati e informazioni su più account. Inoltre, Security Hub viene spesso utilizzato dai clienti che dispongono di un sistema SIEM on-premise, come un preprocessore e aggregatore di avvisi e log lato AWS, da cui possono quindi acquisire Amazon EventBridge tramite un processore e un server di inoltro basati su AWS Lambda.

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

Guida all'implementazione

- Valuta le opzioni per l'elaborazione dei log: valuta le opzioni disponibili per l'elaborazione dei log.
 - [Utilizza Amazon OpenSearch Service per registrare e monitorare \(quasi\) tutto](#)
 - [Individuazione di un partner specializzato in soluzioni di registrazione e monitoraggio](#)
- Come inizio per analizzare i log CloudTrail, testa Amazon Athena.
 - [Configurazione di Athena per analizzare i log CloudTrail.](#)
- Implementa la registrazione centralizzata in AWS: guarda la soluzione di esempio AWS seguente per centralizzare le registrazioni da più origini.
 - [Centralize logging solution](#)
- Implementa la registrazione centralizzata con il partner: i partner APN hanno soluzioni per aiutarti ad analizzare i log centralmente.
 - [Registrazione e Monitoraggio](#)

Risorse

Documenti correlati:

- [AWS Answers: Centralized Logging \(AWS Answers: registrazione centralizzata\)](#)
- [AWS Security Hub](#)
- [Amazon CloudWatch](#)
- [Amazon EventBridge](#)
- [Nozioni di base: Amazon CloudWatch Logs](#)

- [Soluzione dei partner per la sicurezza: registrazione e monitoraggio](#)

Video correlati:

- [Centrally Monitoring Resource Configuration & Compliance](#)
- [Remediating Amazon GuardDuty and AWS Security Hub Findings](#)
- [Threat management in the cloud: Amazon GuardDuty and AWS Security Hub](#)

SEC04-BP03 Automazione delle risposte agli eventi

L'utilizzo dell'automazione per analizzare e correggere gli eventi riduce l'impegno e il rischio di errori umani e consente di dimensionare le capacità di analisi. Le revisioni periodiche ti aiuteranno a ottimizzare gli strumenti di automazione e a effettuare un'iterazione costante.

In AWS, è possibile analizzare gli eventi di interesse e le informazioni relative alle modifiche potenzialmente impreviste in un flusso di lavoro automatizzato utilizzando Amazon EventBridge. Questo servizio fornisce un motore di regole scalabile progettato per gestire sia i formati di eventi AWS nativi (ad esempio eventi AWS CloudTrail), sia gli eventi personalizzati che puoi generare dalla tua applicazione. Amazon GuardDuty consente inoltre di instradare gli eventi a un sistema di flusso di lavoro per i sistemi di risposta agli incidenti (AWS Step Functions), a un account di sicurezza centrale o a un bucket per ulteriori analisi.

È inoltre possibile rilevare le modifiche e instradare queste informazioni al flusso di lavoro corretto utilizzando Regole di AWS Config e [Pacchetti di conformità](#). AWS Config individua le modifiche ai servizi coperti (con una latenza maggiore rispetto a EventBridge) e genera eventi che possono essere analizzati tramite le regole di Regole di AWS Config per il rollback, per rafforzare le policy di conformità e per inviare le informazioni ai sistemi, ad esempio le piattaforme di gestione delle modifiche e i sistemi di ticketing operativi. Oltre a scrivere funzioni Lambda personalizzate per rispondere agli eventi di AWS Config, puoi utilizzare il [kit per lo sviluppo di regole di Regole di AWS Config](#) una [libreria di](#) Regole di AWS Config open source. I pacchetti di conformità sono una raccolta di Regole di AWS Config e di azioni di correzione che distribuisce come entità singola creata come modello YAML. Un [modello di pacchetto di conformità di esempio](#) è disponibile per il Well-Architected Security Pillar.

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

Guida all'implementazione

- Implementa un avviso automatizzato con GuardDuty: 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. Abilita GuardDuty e configura gli avvisi automatici.
- Automatizza i processi di indagine: sviluppa processi automatizzati per indagare su un evento e riferire informazioni a un amministratore per risparmiare tempo.
 - [Laboratorio: Amazon GuardDuty hands on](#)

Risorse

Documenti correlati:

- [AWS Answers: Centralized Logging \(AWS Answers: registrazione centralizzata\)](#)
- [AWS Security Hub](#)
- [Amazon CloudWatch](#)
- [Amazon EventBridge](#)
- [Nozioni di base: Amazon CloudWatch Logs](#)
- [Soluzione dei partner per la sicurezza: registrazione e monitoraggio](#)
- [Configurazione di Amazon GuardDuty](#)

Video correlati:

- [Centrally Monitoring Resource Configuration & Compliance](#)
- [Remediating Amazon GuardDuty and AWS Security Hub Findings](#)
- [Threat management in the cloud: Amazon GuardDuty and AWS Security Hub](#)

Esempi correlati:

- [Laboratorio: Distribuzione automatizzata di controlli di rilevamento](#)

SEC04-BP04 Implementazione di eventi di sicurezza fruibili

Crea e invia al tuo team avvisi fruibili. Assicurati che includano informazioni pertinenti affinché il team possa intervenire. Per ogni meccanismo di rilevamento di cui disponi, devi disporre anche di un processo, sotto forma di [runbook](#) oppure [playbook](#), da analizzare. Ad esempio, quando abiliti [Amazon GuardDuty](#), vengono generati [risultati diversi](#). È necessario disporre di una voce runbook per ogni tipo di risultato; ad esempio, se viene rilevato un [trojan](#), il runbook contiene istruzioni semplici che indicano come eseguire l'analisi e correggere il problema.

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

Guida all'implementazione

- Identificazione delle metriche disponibili per i servizi AWS: scopri le metriche a disposizione attraverso Amazon CloudWatch per i servizi in uso.
 - [Documentazione del servizio AWS](#)
 - [Utilizzare i parametri Amazon CloudWatch](#)
- Configurazione degli avvisi Amazon CloudWatch.
 - [Utilizzo degli allarmi di Amazon CloudWatch](#)

Risorse

Documenti correlati:

- [Amazon CloudWatch](#)
- [Amazon EventBridge](#)
- [Soluzione dei partner per la sicurezza: registrazione e monitoraggio](#)

Video correlati:

- [Centrally Monitoring Resource Configuration & Compliance \(Monitoraggio centrale della configurazione e della conformità delle risorse\)](#)
- [Remediating Amazon GuardDuty and AWS Security Hub Findings \(Correzione Amazon GuardDuty e risultati AWS Security Hub\)](#)
- [Threat management in the cloud: Amazon GuardDuty and AWS Security Hub \(Gestione delle minacce nel cloud: Amazon GuardDuty e AWS Security Hub\)](#)

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 od organizzativi. L'utilizzo di queste metodologie è fondamentale per il successo delle operazioni continuative nel cloud.

La protezione dell'infrastruttura è una parte cruciale di un programma di sicurezza delle informazioni. Assicura infatti che i sistemi e i servizi all'interno del carico di lavoro siano protetti contro gli accessi non intenzionali 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 protezione avanzata, 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 i concetti di Regioni, zone di disponibilità, [Zone locali AWS](#) e [AWS Outposts](#), che rappresentano i componenti dell'infrastruttura globale di sicurezza di AWS.

AWS ha il concetto di una Regione, ossia una sede fisica nel mondo dove riuniamo i data center. Ogni gruppo di data center logici viene definito Zona di disponibilità (AZ). Ogni Regione AWS consiste 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. Ogni AZ dispone di fonti energetiche, sistemi di raffreddamento e sicurezza fisica indipendenti. Se un'applicazione viene suddivisa in più AZ aumentano isolamento e protezione da problematiche come interruzioni dell'alimentazione, colpi di fulmine, 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 una velocità di trasmissione effettiva elevata 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 per essere eseguite in più AZ e raggiungere una tolleranza ai guasti ancora più elevata. Le Regioni AWS soddisfano i più alti 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. Con le Zone locali AWS puoi facilmente eseguire 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. Le Zone locali AWS 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 AWS nativi, infrastrutture e modelli operativi quasi in ogni data center, spazio di co-locazione o struttura on-premise. Puoi usare gli stessi strumenti, le stesse API e le stesse infrastrutture AWS nelle sedi on-premise 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-premise 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 descrivono come utilizzare questi approcci.

Argomenti

- [Protezione delle reti](#)
- [Protezione delle risorse di calcolo](#)

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 dell'applicazione 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 supportati dall'automazione. Analogamente, 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 lo [Approfondimento sulle applicazioni serverless - AWS Well-Architected](#) 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 Automatizzazione della protezione di rete](#)
- [SEC05-BP04 Implementazione di funzioni di ispezione e protezione](#)

SEC05-BP01 Creazione di livelli di rete

Raggruppa i componenti che condividono requisiti di sensibilità in livelli per ridurre al minimo la portata potenziale dell'impatto di un accesso non autorizzato. Ad esempio, un cluster di database in un senza necessità di accesso a Internet deve essere posizionato in sottoreti senza routing da o verso Internet. Il traffico deve provenire solo dalla risorsa adiacente meno sensibile. Considera un'applicazione web che si trova dietro un sistema di bilanciamento del carico. Il tuo database non deve essere accessibile direttamente dal sistema di bilanciamento del carico. Solo il sistema logico aziendale o il server web devono avere accesso diretto al database.

Risultato desiderato: creare una rete stratificata. Le reti a livelli aiutano a raggruppare logicamente componenti di rete simili. Inoltre, riducono la portata potenziale dell'impatto di un accesso non autorizzato alla rete. Una rete adeguatamente stratificata rende più difficile l'accesso a risorse aggiuntive all'interno dell'ambiente AWS da parte di utenti non autorizzati. Oltre a proteggere i percorsi di rete interni, è necessario proteggere anche gli edge di rete, come le applicazioni web e gli endpoint API.

Anti-pattern comuni:

- Creazione di tutte le risorse in un singolo VPC o una singola sottorete.
- Utilizzo di gruppi di sicurezza troppo permissivi.
- Mancato utilizzo di sottoreti.
- Accesso diretto agli archivi di dati, come i database.

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

Guida all'implementazione

Componenti come istanze Amazon Elastic Compute Cloud (Amazon EC2), cluster di database Amazon Relational Database Service (Amazon RDS) e funzioni AWS Lambda che condividono i requisiti di raggiungibilità possono essere segmentati in livelli formati da sottoreti. Considera la possibilità di implementare carichi di lavoro serverless, come le funzioni di [Lambda](#), all'interno di un VPC o dietro un [Amazon API Gateway](#). Le attività di [AWS Fargate \(Fargate\)](#) che non necessitano di accesso a Internet devono essere collocate in sottoreti prive di percorsi da o verso Internet. Questo approccio a più livelli attenua l'impatto di una configurazione a un solo livello errata che può consentire un accesso non intenzionale. Per AWS Lambda è possibile eseguire le funzioni nel proprio VPC per sfruttare i controlli basati sul VPC.

Per una connettività di rete che può includere migliaia di VPC, Account AWS e reti on-premise, è necessario utilizzare [AWS Transit Gateway](#). Transit Gateway agisce come un hub che controlla l'instradamento del traffico tra tutte le reti collegate, che agiscono come raggi. Il traffico tra Amazon Virtual Private Cloud (Amazon VPC) e Transit Gateway rimane sulla rete privata AWS, riducendo così l'esposizione esterna a utenti non autorizzati e a potenziali problemi di sicurezza. Il peering tra regioni di Transit Gateway cripta anche il traffico interregionale, senza un singolo punto di errore o un collo di bottiglia della larghezza di banda.

Passaggi dell'implementazione

- Utilizzare [Reachability Analyzer](#) per analizzare il percorso tra un'origine e una destinazione in base alla configurazione: Reachability Analyzer consente di automatizzare la verifica della connettività da e verso le risorse collegate al VPC. La presente analisi viene eseguita esaminando la configurazione (non vengono inviati pacchetti di rete per condurre l'analisi).
- Utilizzare lo [Strumento di analisi degli accessi alla rete Amazon VPC](#) per identificare l'accesso di rete non intenzionale alle risorse: lo Strumento di analisi degli accessi alla rete Amazon VPC consente di specificare i requisiti di accesso alla rete e di identificare i potenziali percorsi di rete.
- Valutare se le risorse devono trovarsi in una sottorete pubblica: non collocare le risorse nelle sottoreti pubbliche del VPC a meno che non debbano assolutamente ricevere traffico di rete in entrata da origini pubbliche.
- Creare [sottoreti nel VPC](#): crea sottoreti per ogni livello di rete (in gruppi che includono più zone di disponibilità) per migliorare la microsegmentazione. Verifica inoltre di aver associato le [tabelle di instradamento](#) corrette alle sottoreti per controllare l'instradamento e la connettività Internet.

- Utilizzare [AWS Firewall Manager](#) per gestire i gruppi di sicurezza VPC: AWS Firewall Manager contribuisce a ridurre l'onere di gestione derivante dall'uso di più gruppi di sicurezza.
- Utilizzare [AWS WAF](#) per la protezione contro le più comuni vulnerabilità del web: AWS WAF può contribuire a migliorare la sicurezza degli edge ispezionando il traffico alla ricerca di vulnerabilità web comuni, come l'iniezione SQL. Consente inoltre di limitare il traffico da indirizzi IP provenienti da determinati Paesi o aree geografiche.
- Utilizzare [Amazon CloudFront](#) come rete di distribuzione di contenuti (CDN): Amazon CloudFront può contribuire a velocizzare l'applicazione web memorizzando i dati più vicino agli utenti. Può anche migliorare la sicurezza degli edge applicando HTTPS, limitando l'accesso ad aree geografiche e garantendo che il traffico di rete possa accedere alle risorse solo quando viene instradato attraverso CloudFront.
- Utilizzare [Amazon API Gateway](#) per la creazione di interfacce di programmazione delle applicazioni (API): Amazon API Gateway aiuta a pubblicare, monitorare e proteggere le API REST, HTTPS e WebSocket.

Risorse

Documenti correlati:

- [AWS Firewall Manager](#)
- [Amazon Inspector](#)
- [Amazon VPC Security](#) (Sicurezza di Amazon VPC)
- [Reachability Analyzer](#)
- [Strumento di analisi degli accessi alla rete Amazon VPC](#)

Video correlati:

- [AWS Transit Gateway reference architectures for many VPCs](#) (Architetture di riferimento di AWS Transit Gateway per molte VPC)
- [Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield](#) (Accelerazione e protezione delle applicazioni con Amazon CloudFront, AWS WAF e AWS Shield)
- [AWS re:Inforce 2022 - Validate effective network access controls on AWS](#) (re:Inforce 2022: Convalida di controlli di accesso alla rete efficaci su AWS)

- [AWS re:Inforce 2022 - Advanced protections against bots using AWS WAF](#)(AWS re:Inforce 2022 - Protezioni avanzate contro i bot utilizzando AWS WAF)

Esempi correlati:

- [Well-Architected Lab - Automated Deployment of VPC](#) (Well-Architected Lab: Implementazione automatica di VPC)
- [Workshop: Amazon VPC Network Access Analyzer](#) (Workshop: Strumento di analisi degli accessi alla rete Amazon VPC)

SEC05-BP02 Controllo del traffico a tutti i livelli

durante la progettazione della topologia di rete, è necessario esaminare i requisiti di connettività di ciascun componente. Ad esempio, va esaminato se un componente richiede accessibilità a Internet (in entrata e in uscita), connettività a VPC, servizi edge e data center esterni.

Un VPC consente di definire la topologia di rete che si estende su una regione Regione AWS con un intervallo di indirizzi IPv4 privati impostato dall'utente o un intervallo di indirizzi IPv6 selezionato da AWS. È necessario applicare più controlli con un approccio di difesa avanzata sia per il traffico in entrata che per quello in uscita, tra cui l'uso di gruppi di sicurezza (firewall di ispezione stateful), liste di controllo degli accessi di rete, sottoreti e tabelle di routing. All'interno di un VPC, puoi creare sottoreti in una zona di disponibilità. Ogni sottorete può avere una tabella di routing associata che definisce le regole di instradamento per la gestione dei percorsi del traffico all'interno della sottorete. Puoi definire una sottorete Internet instradabile tramite un percorso che va a un gateway Internet o NAT collegato al VPC o attraverso un altro VPC.

Un'istanza, un database Amazon Relational Database Service(Amazon RDS) o un altro servizio che viene avviato all'interno di un VPC ha un proprio gruppo di sicurezza per interfaccia di rete. Questo firewall è esterno al livello del sistema operativo e può essere utilizzato per definire le regole per il traffico consentito in entrata e in uscita. Puoi anche definire le relazioni tra i gruppi di sicurezza. Ad esempio, le istanze all'interno di un gruppo di sicurezza a livello di database accettano solo il traffico dalle istanze all'interno del livello dell'applicazione, in riferimento ai gruppi di sicurezza applicati alle istanze coinvolte. A meno che non utilizzi protocolli non TCP, non dovrebbe essere necessario disporre di un'istanza Amazon Elastic Compute Cloud(Amazon EC2) accessibile direttamente da internet (anche con porte limitate da gruppi di sicurezza) senza un sistema di bilanciamento del carico o [CloudFront](#). Questo aiuta a proteggerla da accessi non intenzionali dovuti a un problema del sistema operativo o dell'applicazione. Una sottorete può anche avere una lista di controllo

degli accessi di rete collegata, che funge da firewall stateless. È necessario configurare la lista di controllo degli accessi di rete per limitare l'ambito del traffico consentito tra i livelli; tieni presente che è necessario definire le regole sia in entrata che in uscita.

Alcuni servizi AWS richiedono dei componenti per accedere a internet per le chiamate API, in cui [si trovano gli endpoint API AWS](#). Altri servizi AWS usano [Endpoint VPC](#) all'interno dei Amazon VPC. Molti servizi AWS, tra cui Amazon S3 e Amazon DynamoDB, supportano gli endpoint VPC e questa tecnologia è stata generalizzata in [AWS PrivateLink](#). Ti consigliamo di usare questo approccio per accedere ai servizi AWS, ai servizi di terze parti e ai servizi proprietari ospitati in sicurezza in altri VPC. Tutto il traffico di rete su AWS PrivateLink rimane sul backbone AWS globale e non attraversa mai internet. La connettività può solo essere avviata dal consumatore del servizio e non dal provider del servizio. Usando l'accesso AWS PrivateLink per i servizi esterni è possibile creare VPC isolati senza accesso a internet e proteggere i VPC da vettori di minacce esterni. I servizi di terze parti possono usare AWS PrivateLink per consentire ai propri clienti di connettersi ai servizi dai propri VPC su indirizzi IP privati. Per gli asset del VPC che devono effettuare connessioni in uscita a Internet, queste possono essere effettuate solo in uscita (unidirezionale) tramite un gateway NAT gestito da AWS, un gateway Internet per connessioni solo in uscita o proxy Web creati e gestiti dall'utente.

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

Guida all'implementazione

- Controlla il traffico di rete in un VPC: implementa le best practice di VPC per controllare il traffico.
 - [Sicurezza Amazon VPC](#)
 - [Endpoint VPC](#)
 - [Gruppo di sicurezza Amazon VPC](#)
 - [ACL di rete](#)
- Controlla il traffico a livello di edge: implementa servizi edge, come Amazon CloudFront, per fornire un ulteriore livello di protezione e altre funzionalità.
 - [Casi d'uso Amazon CloudFront](#)
 - [AWS Global Accelerator](#)
 - [AWS Web Application Firewall \(AWS WAF\)](#)
 - [Amazon Route 53](#)
 - [Amazon VPC Ingress Routing](#)
- Controlla il traffico di rete privato: implementa servizi in grado di proteggere il traffico privato per il carico di lavoro.

- [Amazon VPC Peering](#)
- [Amazon VPC Endpoint Services \(AWS PrivateLink\)](#)
- [Amazon VPC Transit Gateway](#)
- [AWS Direct Connect](#)
- [AWS Site-to-Site VPN](#)
- [AWS Client VPN](#)
- [Amazon S3 Access Points](#)

Risorse

Documenti correlati:

- [AWS Firewall Manager](#)
- [Amazon Inspector](#)
- [Nozioni di base su AWS WAF](#)

Video correlati:

- [AWS Transit Gateway reference architectures for many VPCs](#)
- [Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield](#)

Esempi correlati:

- [Laboratorio: Distribuzione automatizzata di VPC](#)

SEC05-BP03 Automatizzazione della protezione di rete

Automatizza i meccanismi di protezione per creare una rete in grado di difendersi da sola grazie alle informazioni sulle minacce e al rilevamento delle anomalie. Ad esempio, strumenti di rilevamento e prevenzione delle intrusioni in grado di adattarsi alle minacce attuali e di ridurre il loro impatto. Un firewall per applicazioni Web è un esempio di dove è possibile automatizzare la protezione della rete, ad esempio utilizzando la soluzione Automatismi di sicurezza di AWS WAF (<https://github.com/awslabs/aws-waf-security-automations>) per bloccare automaticamente le richieste provenienti da indirizzi IP associati a noti attori di minacce.

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

Guida all'implementazione

- Automatizza la protezione per il traffico basato sul Web: AWS offre una soluzione che usa AWS CloudFormation per distribuire automaticamente una serie di regole AWS WAF progettate per filtrare gli attacchi comuni basati sul Web. Gli utenti hanno la possibilità di scegliere tra caratteristiche di protezione preconfigurate che definiscono le regole incluse in una lista di controllo accessi Web (ACL Web) di AWS WAF.
 - [Automazioni di sicurezza AWS WAF](#)
- Considera le soluzioni AWS Partner: i partner AWS offrono centinaia di prodotti leader nel settore che sono equivalenti, identici o si integrano ai controlli esistenti negli ambienti on-premise. Questi prodotti integrano i servizi AWS esistenti per permettere di distribuire un'architettura di sicurezza completa e un'esperienza più fluida nel cloud e negli ambienti on-premise.
 - [Sicurezza dell'infrastruttura](#)

Risorse

Documenti correlati:

- [AWS Firewall Manager](#)
- [Amazon Inspector](#)
- [Sicurezza di Amazon VPC](#)
- [Nozioni di base su AWS WAF](#)

Video correlati:

- [AWS Transit Gateway reference architectures for many VPCs](#)
- [Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield](#)

Esempi correlati:

- [Laboratorio: Distribuzione automatizzata di VPC](#)

SEC05-BP04 Implementazione di funzioni di ispezione e protezione

Ispeziona e filtra il traffico a ogni livello. Puoi ispezionare le configurazioni VPC per rilevare potenziali accessi indesiderati con [VPC Network Access Analyzer](#). Puoi specificare i requisiti di accesso alla rete e individuare percorsi di rete potenziali che non li soddisfano. Per i componenti che eseguono transazioni tramite protocolli basati su HTTP, un firewall per applicazioni Web può aiutare a proteggere dagli attacchi comuni. [AWS WAF](#) è un firewall per applicazioni Web che consente di monitorare e bloccare le richieste HTTP che corrispondono alle regole configurabili inoltrate a un'API di Amazon API Gateway, ad Amazon CloudFront o a un Application Load Balancer. Per iniziare a usare AWS WAF, puoi utilizzare [Regole gestite da AWS](#) in combinazione con le tue oppure puoi utilizzare [integrazioni dei partner esistenti](#).

Per gestire le protezioni di AWS WAF, AWS Shield Advanced e i gruppi di sicurezza di Amazon VPC in AWS Organizations, puoi utilizzare AWS Firewall Manager. Questo consente di configurare e gestire centralmente le regole del firewall tra gli account e le applicazioni, rendendo più semplice il dimensionamento dell'applicazione delle regole comuni. Consente inoltre di rispondere rapidamente agli attacchi utilizzando [AWS Shield Advanced soluzioni](#) che bloccano automaticamente le richieste indesiderate alle applicazioni Web. Firewall Manager funziona anche con [AWS Network Firewall](#). AWS Network Firewall è un servizio gestito che usa un motore di regole per garantire un controllo granulare sul traffico di rete stateful e stateless. Supporta le specifiche [dell'intrusion prevention system \(IPS\)](#) open source compatibile con Suricata per le regole che contribuiscono alla protezione del carico di lavoro.

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

Guida all'implementazione

- Configura Amazon GuardDuty: 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 Account AWS. Abilita GuardDuty e configura gli avvisi automatici.
 - [Amazon GuardDuty](#)
 - [Laboratorio: Distribuzione automatizzata di controlli di rilevamento](#)
- Configura i log di flusso del cloud privato virtuale (VPC): Log di flusso VPC è una funzione che ti permette di acquisire informazioni sul traffico IP in entrata e in uscita dalle interfacce di rete nel tuo VPC. I dati del log di flusso possono essere pubblicati su Amazon CloudWatch Logs e Amazon Simple Storage Service (Amazon S3). Dopo aver creato un log di flusso, puoi recuperarne e visualizzarne i dati nella destinazione scelta.

- Considera il mirroring del traffico VPC: il mirroring del traffico è una caratteristica di Amazon VPC che puoi utilizzare per copiare il traffico di rete da un'interfaccia di rete elastica di istanze Amazon Elastic Compute Cloud (Amazon EC2) e quindi inviarlo ad appliance di sicurezza e monitoraggio fuori banda per l'ispezione dei contenuti, il monitoraggio delle minacce e la risoluzione dei problemi.
 - [Mirroring del traffico del VPC](#)

Risorse

Documenti correlati:

- [AWS Firewall Manager](#)
- [Amazon Inspector](#)
- [Sicurezza Amazon VPC](#)
- [Nozioni di base su AWS WAF](#)

Video correlati:

- [AWS Transit Gateway reference architectures for many VPCs](#)
- [Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield](#)

Esempi correlati:

- [Laboratorio: Distribuzione automatizzata di VPC](#)

Protezione delle risorse di calcolo

Le risorse di calcolo includono istanze EC2, container, funzioni di AWS Lambda, servizi di database, dispositivi IoT e altro. Ognuno di questi tipi di risorse di calcolo richiede approcci di sicurezza diversi. Tuttavia, condividono strategie comuni che devi 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 ogni servizio AWS utilizzato è importante verificare i suggerimenti di sicurezza specifici nella documentazione del servizio.

Best practice

- [SEC06-BP01 Gestione delle vulnerabilità](#)

- [SEC06-BP02 Riduzione della superficie d'attacco](#)
- [SEC06-BP03 Implementazione di servizi gestiti](#)
- [SEC06-BP04 Automatizzazione della protezione delle risorse di calcolo](#)
- [SEC06-BP05 Concessione del permesso di eseguire azioni a distanza](#)
- [SEC06-BP06 Convalida dell'integrità del software](#)

SEC06-BP01 Gestione delle vulnerabilità

Scansiona e correggi frequentemente le vulnerabilità del codice, delle dipendenze e dell'infrastruttura per proteggere da nuove minacce.

Risultato desiderato: creare e mantenere un programma di gestione delle vulnerabilità. Esegui regolarmente scansioni e patch su risorse quali istanze Amazon EC2, container Amazon Elastic Container Service (Amazon ECS) e carichi di lavoro Amazon Elastic Kubernetes Service (Amazon EKS). Configura finestre di manutenzione per le risorse gestite da AWS, come i database Amazon Relational Database Service (Amazon RDS). Utilizza la scansione statica del codice per ispezionare il codice sorgente delle applicazioni alla ricerca di problemi comuni. Considera la possibilità di effettuare test di penetrazione (pen-test) delle applicazioni web se l'organizzazione dispone delle competenze necessarie o se può avvalersi di un'assistenza esterna.

Anti-pattern comuni:

- Assenza di un programma di gestione delle vulnerabilità.
- Esecuzione di patch di sistema senza considerare la gravità o la 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.

Vantaggi dell'adozione di questa best practice:

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

Guida all'implementazione

Un programma di gestione delle vulnerabilità comprende la valutazione della sicurezza, l'identificazione dei problemi, la definizione delle priorità e l'esecuzione di operazioni di patch per risolvere i problemi. L'automazione è la chiave per la scansione continua dei carichi di lavoro alla ricerca di problemi e di esposizioni di rete non intenzionali e per l'esecuzione di interventi correttivi.

L'automazione della creazione e dell'aggiornamento delle risorse fa risparmiare tempo e riduce il rischio che gli errori di configurazione creino ulteriori problemi. Un programma di gestione delle vulnerabilità ben progettato dovrebbe considerare anche la verifica delle vulnerabilità durante le fasi di sviluppo e implementazione del ciclo di vita del software. L'implementazione della gestione delle vulnerabilità durante lo sviluppo e la distribuzione aiuta a ridurre le possibilità che una vulnerabilità si diffonda nell'ambiente di produzione.

L'implementazione di un programma di gestione delle vulnerabilità richiede una buona conoscenza del [Modello di responsabilità condivisa di AWS](#) e del suo rapporto con i carichi di lavoro specifici. Secondo tale modello, AWS è responsabile della protezione dell'infrastruttura del Cloud AWS. Questa infrastruttura è composta da hardware, software, reti e strutture che eseguono i servizi Cloud AWS. La responsabilità della sicurezza nel cloud spetta a te, ad esempio per quanto riguarda i dati effettivi, la configurazione della sicurezza, le attività di gestione delle istanze Amazon EC2 e la verifica che gli oggetti Amazon S3 siano classificati e configurati correttamente. L'approccio alla gestione delle vulnerabilità può variare anche in base ai servizi utilizzati. Ad esempio, AWS gestisce l'applicazione di patch per il nostro servizio di database relazionale gestito Amazon RDS, ma tu sei responsabile dell'applicazione di patch dei database autogestiti.

AWS offre una serie di servizi per la gestione delle vulnerabilità [Amazon Inspector](#) esegue continuamente la scansione dei carichi di lavoro AWS alla ricerca di problemi software e di accessi di rete non intenzionali. [AWS Systems Manager Patch Manager](#) supporta la gestione dell'applicazione di patch sulle istanze Amazon EC2. Amazon Inspector e Systems Manager possono essere visualizzati in [AWS Security Hub](#), un servizio di gestione della postura di sicurezza del cloud che aiuta ad automatizzare i controlli di sicurezza AWS e a centralizzare gli avvisi di sicurezza.

[Amazon CodeGuru](#) può aiutare a identificare potenziali problemi nelle applicazioni Java e Python utilizzando l'analisi statica del codice.

Passaggi dell'implementazione

- Configurare [Amazon Inspector](#): Amazon Inspector rileva automaticamente le istanze Amazon EC2 appena lanciate, le funzioni Lambda e le immagini di container idonee inviate ad Amazon ECR e le analizza immediatamente alla ricerca di problemi di software, potenziali difetti ed esposizione di rete non intenzionale.
- Eseguire la scansione del codice sorgente: esegui la scansione delle librerie e delle dipendenze alla ricerca di problemi e difetti. [Amazon CodeGuru](#) può scansionare e fornire consigli per risolvere i [problemi di sicurezza più comuni](#) per le applicazioni Java e Python. [OWASP Foundation](#) pubblica un elenco di strumenti per l'analisi del codice sorgente (noti anche come strumenti SAST).

- Implementare un processo che consenta di eseguire la scansione dell'ambiente e di applicarvi le patch, nonché di eseguire la scansione come parte di un processo di compilazione di una pipeline CI/CD: implementa un processo per la scansione e l'applicazione di patch per i problemi delle dipendenze e dei sistemi operativi per proteggerti dalle nuove minacce. Tale processo deve essere eseguito regolarmente. La gestione delle vulnerabilità del software è essenziale per capire dove è necessario applicare le patch o risolvere i problemi del software. Stabilisci le priorità per la correzione di potenziali problemi di sicurezza incorporando le valutazioni di vulnerabilità nelle fasi iniziali della pipeline di integrazione continua/consegna continua (CI/ CD). L'approccio può variare in base ai servizi AWS utilizzati. Per verificare la presenza di potenziali problemi nel software in esecuzione nelle istanze Amazon EC2, aggiungi [Amazon Inspector](#) alla pipeline per avvisare l'utente e interrompere il processo di creazione se vengono rilevati problemi o potenziali difetti. Amazon Inspector monitora le risorse in modo continuo. Puoi anche utilizzare i prodotti open source come [OWASP Dependency-Check](#), [Snyk](#), [OpenVAS](#), i sistemi di gestione dei pacchetti e gli strumenti AWS Partner per la gestione delle vulnerabilità.
- Utilizza [AWS Systems Manager](#): sei responsabile della gestione delle patch per le risorse AWS, incluse le istanze Amazon Elastic Compute Cloud (Amazon EC2), le Amazon Machine Image (AMI) e le altre risorse di calcolo. [AWS Systems Manager Patch Manager](#) automatizza il processo di patch delle istanze gestite con aggiornamenti di sicurezza e di altro tipo. Patch Manager può essere utilizzato per applicare le patch alle istanze Amazon EC2 sia per i sistemi operativi che per le applicazioni, inclusi applicazioni Microsoft, service pack di Windows e aggiornamenti di versione minori per le istanze basate su Linux. Oltre a Amazon EC2, Patch Manager può essere utilizzato anche per applicare patch ai server on-premise.

Per avere un elenco dei sistemi operativi supportati, consulta [Sistemi operativi supportati](#) nella Guida per l'utente di Systems Manager. Puoi eseguire la scansione delle istanze per visualizzare solo un report delle patch mancanti oppure puoi eseguire la scansione e installare automaticamente tutte le patch mancanti.

- Utilizzare [AWS Security Hub](#): Security Hub offre una visione completa dello stato di sicurezza in AWS. Raccoglie i dati di sicurezza su [più servizi AWS](#) e fornisce tali risultati in un formato standardizzato, consentendo di dare priorità ai risultati della sicurezza tra i servizi AWS.
- Utilizzare [AWS CloudFormation](#): [AWS CloudFormation](#) è un servizio Infrastruttura come codice (IaC) che può essere d'aiuto nella gestione delle vulnerabilità, automatizzando l'implementazione delle risorse e standardizzando l'architettura delle risorse tra più account e ambienti.

Risorse

Documenti correlati:

- [AWS Systems Manager](#)
- [Security Overview of AWS Lambda](#) (Panoramica sulla sicurezza di AWS Lambda)
- [Amazon CodeGuru](#)
- [Improved, Automated Vulnerability Management for Cloud Workloads with a New Amazon Inspector](#) (Gestione delle vulnerabilità migliorata e automatizzata per i carichi di lavoro cloud con un nuovo Amazon Inspector)
- [Automate vulnerability management and remediation in AWS using Amazon Inspector and AWS Systems Manager – Part 1](#) (Automatizzare la gestione delle vulnerabilità e la bonifica in AWS utilizzando Amazon Inspector e AWS Systems Manager - Parte 1)

Video correlati:

- [Securing Serverless and Container Services](#)
- [Security best practices for the Amazon EC2 instance metadata service](#) (Best practice di sicurezza per il servizio di metadati dell'istanza Amazon EC2)

SEC06-BP02 Riduzione della superficie d'attacco

Riduci la superficie di attacco ad accessi non intenzionali attraverso la protezione avanzata dei sistemi operativi e riducendo al minimo i componenti, le librerie e i servizi di consumo esterni in uso. Inizia riducendo i componenti inutilizzati, siano essi pacchetti del sistema operativo o applicazioni per carichi di lavoro basati su Amazon Elastic Compute Cloud (Amazon EC2) o moduli software esterni nel codice (per tutti i carichi di lavoro). Esistono molte guide per la configurazione della protezione avanzata e della sicurezza dei sistemi operativi e dei software dei server comuni. Ad esempio, puoi iniziare dal [Center for Internet Security](#) e iterare.

In Amazon EC2 puoi creare Amazon Machine Image (AMI), con patch e rafforzamento, per soddisfare i requisiti di sicurezza specifici della tua organizzazione. Le patch e altri controlli di sicurezza che applichi sulle AMI diventano effettivi nel momento in cui vengono creati: non sono dinamici, a meno che tu non decida di modificarli subito dopo l'avvio, ad es. con AWS Systems Manager.

Puoi semplificare il processo di creazione di AMI sicure con EC2 Image Builder. EC2 Image Builder riduce in modo significativo l'impegno richiesto per creare e mantenere immagini "golden" senza scrivere e aggiornare la manutenzione. Quando sono disponibili gli aggiornamenti software, Image Builder produce automaticamente una nuova immagine senza richiedere agli utenti di iniziare una creazione manuale. EC2 Image Builder consente di convalidare con facilità la funzionalità e la sicurezza delle immagini prima di usarle in produzione con test tuoi e forniti da AWS. Puoi anche applicare impostazioni di sicurezza fornite da AWS per proteggere ulteriormente le immagine e rispettare i criteri di sicurezza interni. Ad esempio, puoi produrre immagini conformi allo standard Security Technical Implementation Guide (STIG) con modelli forniti da AWS.

Con l'utilizzo di strumenti di analisi del codice statico di terze parti puoi identificare problemi di sicurezza comuni, ad esempio limiti di input delle funzioni non controllati e CVE applicabili. Puoi utilizzare [Amazon CodeGuru](#) per le lingue supportate. Possono anche essere utilizzati strumenti di controllo delle dipendenze per stabilire se le librerie a cui si collega il codice sono le versioni più recenti, se le stesse sono prive di CVE e se le condizioni di licenza soddisfano i requisiti delle policy del software.

Con Amazon Inspector puoi eseguire valutazioni della configurazione a fronte delle istanze per CVE note, confrontare i valori rispetto a benchmark di sicurezza e automatizzare la notifica dei difetti. Amazon Inspector viene eseguito sulle istanze di produzione o in una pipeline di compilazione e invia una notifica agli sviluppatori e agli ingegneri quando sono disponibili nuovi risultati. Puoi accedere in modo programmatico ai risultati e indirizzare i tuoi team ai sistemi di backlog e rilevamento dei bug. [EC2 Image Builder](#) può essere utilizzato per mantenere le immagini del server (AMI) tramite l'applicazione di patch automatizzata, l'applicazione di policy di sicurezza fornite da AWS e altre personalizzazioni. Quando utilizzi i container, implementa la [scansione delle immagini ECR](#) nella pipeline di compilazione regolarmente confrontandola con il repository di immagini per cercare le CVE nei container.

Anche se Amazon Inspector e altri strumenti sono efficaci per identificare configurazioni ed eventuali CVE presenti, sono necessari altri metodi per testare il carico di lavoro a livello di applicazione. [Il fuzzing](#) è un metodo noto di individuazione dei bug mediante l'automazione per inserire dati malformati nei campi di input e in altre aree dell'applicazione.

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

Guida all'implementazione

- Rafforzamento del sistema operativo: configura i sistemi operativi per adeguarli alle best practice.
 - [Protezione di Amazon Linux](#)

- [Protezione di Microsoft Windows Server](#)
- Rafforzamento delle risorse containerizzate: configura le risorse containerizzate per la conformità alle best practice in materia di sicurezza.
- Implementa le best practice AWS Lambda.
 - [Best practice di AWS Lambda](#)

Risorse

Documenti correlati:

- [AWS Systems Manager](#)
- [Sostituzione di un host bastione con Amazon EC2 Systems Manager](#)
- [Panoramica sulla sicurezza di AWS Lambda](#)

Video correlati:

- [Esecuzione di carichi di lavoro con livello di sicurezza elevato su Amazon EKS](#)
- [Securing Serverless and Container Services](#)
- [Best practice di sicurezza per il servizio di metadati dell'istanza Amazon EC2](#)

Esempi correlati:

- [Laboratorio: Distribuzione automatizzata di firewall per applicazioni Web](#)

SEC06-BP03 Implementazione di servizi gestiti

Implementa servizi che gestiscono le risorse, ad esempio Amazon Relational Database Service (Amazon RDS), AWS Lambda e Amazon Elastic Container Service (Amazon ECS), per ridurre le attività di manutenzione della sicurezza nell'ambito del modello di responsabilità condivisa. Ad esempio, Amazon RDS aiuta a configurare, gestire e dimensionare un database relazionale e automatizza le attività di amministrazione quali provisioning di hardware, configurazione di database, applicazione di patch e backup. Ciò significa che hai più tempo libero per concentrarti sulla protezione dell'applicazione in altri modi descritti nel Framework AWS Well-Architected. Lambda consente di eseguire il codice senza dover effettuare il provisioning o gestire server, perciò è sufficiente

focalizzarsi su connettività, invocazione e sicurezza a livello di codice, anziché sull'infrastruttura o sul sistema operativo.

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

Guida all'implementazione

- Identificazione dei servizi disponibili: esplora, testa e implementa servizi che gestiscono le risorse, come Amazon RDS, AWS Lambda e Amazon ECS.

Risorse

Documenti correlati:

- [Sito Web AWS](#)
- [AWS Systems Manager](#)
- [Sostituzione di un host bastione con Amazon EC2 Systems Manager](#)
- [Panoramica sulla sicurezza di AWS Lambda](#)

Video correlati:

- [Esecuzione di carichi di lavoro con livello di sicurezza elevato su Amazon EKS](#)
- [Securing Serverless and Container Services](#)
- [Best practice di sicurezza per il servizio di metadati dell'istanza Amazon EC2](#)

Esempi correlati:

- [Laboratorio: Richiesta di certificati pubblici da parte di Gestione certificati AWS](#)

SEC06-BP04 Automatizzazione della protezione delle risorse di calcolo

Automatizza i meccanismi di protezione delle risorse di calcolo, tra cui la gestione delle vulnerabilità, la riduzione della superficie di attacco e la gestione delle risorse. L'automazione ti consentirà di investire tempo nella protezione di altri aspetti del carico di lavoro e di ridurre il rischio di errori umani.

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

Guida all'implementazione

- Automazione della gestione della configurazione: applica e convalida in automatico configurazioni sicure sfruttando un apposito servizio o strumento di gestione.
 - [AWS Systems Manager](#)
 - [AWS CloudFormation](#)
 - [Laboratorio: Implementazione automatizzata di VPC](#)
 - [Laboratorio: Implementazione automatizzata di applicazioni Web EC2](#)
- Automazione dell'applicazione delle patch alle istanze Amazon Elastic Compute Cloud (Amazon EC2): AWS Systems Manager Patch Manager automatizza il processo di applicazione di patch alle istanze gestite con aggiornamenti correlati alla sicurezza e di altro tipo. Puoi utilizzare il gestore patch per applicare patch sia per i sistemi operativi sia per le applicazioni.
 - [AWS Systems Manager Patch Manager](#)
 - [Applicazione di patch centralizzata multi-regione e multi-account con AWS Systems Manager Automation.](#)
- Implementazione della prevenzione e del rilevamento delle intrusioni: implementa uno strumento di rilevamento e prevenzione delle intrusioni per monitorare e bloccare le attività sospette sulle istanze.
- Considerazione delle soluzioni AWS Partner: i partner AWS offrono centinaia di prodotti leader nel settore che sono equivalenti, identici o si integrano ai controlli esistenti negli ambienti on-premise. Questi prodotti integrano i servizi AWS esistenti per permettere di implementare un'architettura di sicurezza completa e un'esperienza più fluida nel cloud e negli ambienti on-premise.
 - [Sicurezza dell'infrastruttura](#)

Risorse

Documenti correlati:

- [AWS CloudFormation](#)
- [AWS Systems Manager](#)
- [AWS Systems Manager Patch Manager](#)

- [Applicazione di patch centralizzata multi-regione e multi-account con AWS Systems Manager Automation.](#)
- [Sicurezza dell'infrastruttura](#)
- [Sostituzione di un host bastione con Amazon EC2 Systems Manager](#)
- [Panoramica sulla sicurezza di AWS Lambda](#)

Video correlati:

- [Esecuzione di carichi di lavoro con livello di sicurezza elevato su Amazon EKS](#)
- [Securing Serverless and Container Services](#)
- [Best practice di sicurezza per il servizio di metadati dell'istanza Amazon EC2](#)

Esempi correlati:

- [Laboratorio: Implementazione automatizzata di firewall per applicazioni Web](#)
- [Laboratorio: Implementazione automatizzata di applicazioni Web EC2](#)

SEC06-BP05 Concessione del permesso di eseguire azioni a distanza

Eliminare la possibilità di accesso interattivo riduce il rischio di errore umano e la potenziale configurazione o gestione manuale. Ad esempio, utilizza un flusso di lavoro per la gestione delle modifiche per distribuire le istanze Amazon Elastic Compute Cloud (Amazon EC2) tramite infrastructure-as-code, quindi gestire le istanze Amazon EC2 utilizzando strumenti come AWS Systems Manager invece di consentire l'accesso diretto o tramite un host bastione. AWS Systems Manager può automatizzare un'ampia gamma di attività di manutenzione e distribuzione utilizzando funzionalità quali [automazione di automazione](#), [documenti](#) (playbook) e il [Run Command](#). Gli stack di AWS CloudFormation si basano su pipeline e possono automatizzare le attività di distribuzione e gestione dell'infrastruttura senza utilizzare direttamente la AWS Management Console o le API.

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

Guida all'implementazione

- Sostituisci l'accesso della console: sostituisci l'accesso via console (SSH o RDP) alle istanze con AWS Systems Manager Run Command per automatizzare le attività di gestione.

- [AWS Systems Manager Run Command](#)

Risorse

Documenti correlati:

- [AWS Systems Manager](#)
- [AWS Systems Manager Run Command](#)
- [Sostituzione di un host bastione con Amazon EC2 Systems Manager](#)
- [Panoramica sulla sicurezza di AWS Lambda](#)

Video correlati:

- [Esecuzione di carichi di lavoro con livello di sicurezza elevato su Amazon EKS](#)
- [Securing Serverless and Container Services](#)
- [Best practice di sicurezza per il servizio di metadati dell'istanza Amazon EC2](#)

Esempi correlati:

- [Laboratorio: Distribuzione automatizzata di firewall per applicazioni Web](#)

SEC06-BP06 Convalida dell'integrità del software

Implementa meccanismi (ad esempio la firma del codice) per verificare che il software, il codice e le librerie utilizzati nel carico di lavoro provengano da origini attendibili e non siano stati manomessi. Ad esempio, devi verificare il certificato di firma del codice dei file binari e degli script per confermare l'autore e accertarti che non sia stato manomesso da quando è stato creato dall'autore. [AWS Signer](#) può aiutare a garantire l'affidabilità e l'integrità del tuo codice tramite una sua gestione centralizzata, registrando il ciclo di vita, incluso la registrazione delle certificazioni e delle chiavi pubbliche e private. Puoi imparare come usare modelli avanzati e best practice per la registrazione del codice con [AWS Lambda](#). Inoltre, un confronto tra il checksum del software scaricato e quello del provider può garantire che non sia stato manomesso.

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

Guida all'implementazione

- Analizza i meccanismi: la firma del codice è uno dei meccanismi utili per convalidare l'integrità del software.
 - [NIST: considerazioni sulla sicurezza per la registrazione del codice](#)

Risorse

Documenti correlati:

- [AWS Signer](#)
- [Nuovo – Code Signing, a Trust and Integrity Control for AWS Lambda](#)

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](#)
- [Protezione dei dati inattivi](#)
- [Protezione dei dati in transito](#)

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 Identificazione dei dati all'interno del carico di lavoro](#)
- [SEC07-BP02 Definizione dei controlli di protezione dei dati](#)
- [SEC07-BP03 Automazione dell'identificazione e della classificazione](#)
- [SEC07-BP04 Definizione della gestione del ciclo di vita dei dati](#)

SEC07-BP01 Identificazione dei dati all'interno del carico di lavoro

Comprendere il tipo e la classificazione dei dati che il carico di lavoro elabora, i processi aziendali associati, il luogo in cui i dati sono archiviati e chi è il proprietario dei dati è fondamentale. Occorre inoltre conoscere i requisiti legali e di conformità applicabili al proprio carico di lavoro e i controlli sui dati che devono essere applicati. L'identificazione dei dati è il primo passo nel percorso della classificazione dei dati.

Vantaggi dell'adozione di questa best practice:

La classificazione dei dati consente ai proprietari dei carichi di lavoro di identificare le posizioni in cui sono memorizzati i dati sensibili e di determinare le modalità di accesso e condivisione di tali dati.

La classificazione dei dati mira a rispondere alle seguenti domande:

- Che tipo di dati abbiamo?

Si può trattare di dati quali:

- Proprietà intellettuale (IP) come segreti commerciali, brevetti o accordi contrattuali.
- Informazioni sanitarie protette (PHI), come le cartelle cliniche che contengono informazioni sulla storia medica di un individuo.
- Informazioni di identificazione personale (PII), quali nome, indirizzo, data di nascita e numero di identificazione o registrazione nazionale.
- Dati della carta di credito, come il numero di conto primario (PAN), il nome del titolare della carta, la data di scadenza e il numero del codice di servizio.
- Dove sono archiviati i dati sensibili?
- Chi può accedervi, modificarli e cancellarli?
- Comprendere le autorizzazioni degli utenti è essenziale per prevenire una potenziale gestione errata dei dati.
- Chi può eseguire operazioni di creazione, lettura, aggiornamento e cancellazione (CRUD)?
 - Considerare la potenziale escalation di privilegi comprendendo chi può gestire le autorizzazioni per i dati.
- Quale impatto aziendale può verificarsi se i dati vengono divulgati involontariamente, alterati o cancellati?
 - Comprendere le conseguenze del rischio in caso di modifica, cancellazione o divulgazione involontaria dei dati.

Conoscendo le risposte a queste domande, puoi intraprendere le seguenti azioni:

- Ridurre la portata dei dati sensibili (ad esempio il numero di posizioni dei dati sensibili) e limitare l'accesso ai dati sensibili solo agli utenti autorizzati.
- Acquisire consapevolezza dei diversi tipi di dati in modo da poter implementare meccanismi e tecniche di protezione dei dati appropriati, come la crittografia, la prevenzione della perdita di dati e la gestione dell'identità e degli accessi.

- Ottimizzare i costi fornendo i giusti obiettivi di controllo per i dati.
- Rispondere con sicurezza alle domande delle autorità di regolamentazione e dei revisori in merito ai tipi e alla quantità di dati e al modo in cui i dati di diversa sensibilità vengono isolati l'uno dall'altro.

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

Guida all'implementazione

La classificazione dei dati è l'atto di identificare la sensibilità dei dati. Può essere necessaria l'applicazione di tag per rendere i dati facilmente ricercabili e rintracciabili. La classificazione dei dati riduce anche la loro duplicazione, contribuendo a ridurre i costi di archiviazione e di backup e accelerando il processo di ricerca.

Utilizza servizi come Amazon Macie per automatizzare su larga scala sia la scoperta che la classificazione dei dati sensibili. Altri servizi, quali Amazon EventBridge e AWS Config, possono essere utilizzati per automatizzare la correzione dei problemi di sicurezza dei dati, ad esempio i bucket Amazon Simple Storage Service (Amazon S3) e i volumi EBS Amazon EC2 non crittografati o le risorse di dati prive di tag. Per un elenco completo di integrazioni del servizio AWS, consulta la [Documentazione di EventBridge](#).

Il [rilevamento di PII](#) nei dati non strutturati, come le e-mail dei clienti, i ticket di assistenza, le recensioni dei prodotti e i social media è possibile [mediante Amazon Comprehend](#), che è un servizio di elaborazione del linguaggio naturale (NLP) che utilizza il machine learning per trovare approfondimenti e relazioni come persone, luoghi, sentimenti e argomenti in testi non strutturati. Per l'elenco di servizi AWS che possono aiutare nell'identificazione dei dati, consulta [Common techniques to detect PHI and PII data using AWS services](#) (Tecniche comuni per rilevare i dati PHI e PII utilizzando i servizi AWS).

Un altro metodo che supporta la classificazione e la protezione dei dati è l'[applicazione di tag alle risorse AWS](#). L'applicazione di tag consente di assegnare metadati alle risorse AWS che possono essere utilizzati per gestire, identificare, organizzare, cercare e filtrare le risorse.

In alcuni casi, puoi scegliere di applicare tag a intere risorse (come un bucket S3), soprattutto quando è previsto che un carico di lavoro o un servizio specifico memorizzi processi o trasmissioni di dati di classificazione già nota.

Se necessario, è possibile applicare tag a un bucket S3 anziché i singoli oggetti per semplificare l'amministrazione e la manutenzione della sicurezza.

Passaggi dell'implementazione

Rilevare i dati sensibili all'interno di Amazon S3:

1. Prima di iniziare, verifica di disporre delle autorizzazioni appropriate per accedere alla console Amazon Macie e alle operazioni API. Per dettagli aggiuntivi, consulta [Getting started with Amazon Macie](#) (Nozioni di base su Amazon Macie).
2. Utilizza Amazon Macie per eseguire il rilevamento automatico dei dati quando i dati sensibili risiedono in [Amazon S3](#).
 - Utilizza la guida [Getting Started with Amazon Macie](#) per configurare un repository per i risultati del rilevamento dei dati sensibili e creare un lavoro di rilevamento per i dati sensibili.
 - [How to use Amazon Macie to preview sensitive data in S3 buckets](#) (Come utilizzare Amazon Macie per visualizzare in anteprima i dati sensibili nei bucket S3).

Per impostazione predefinita, Macie analizza gli oggetti utilizzando il set di identificatori di dati gestiti che raccomandiamo per il rilevamento automatico dei dati sensibili. Puoi personalizzare l'analisi configurando Macie in modo che utilizzi specifici identificatori di dati gestiti, identificatori di dati personalizzati ed elenchi di permessi quando esegue il rilevamento automatico di dati sensibili per l'account o l'organizzazione. Puoi regolare l'ambito dell'analisi escludendo bucket specifici (ad esempio, i bucket S3 che di solito memorizzano i dati di registrazione AWS).

3. Per configurare e utilizzare l'individuazione automatica dei dati sensibili, consulta [Performing automated sensitive data discovery with Amazon Macie](#) (Eseguire un rilevamento automatizzato dei dati sensibili con Amazon Macie).
4. Puoi anche considerare [Automated Data Discovery for Amazon Macie](#) (Rilevamento automatizzato dei dati per Amazon Macie).

Rilevare i dati sensibili all'interno di Amazon RDS:

Per ulteriori informazioni sul rilevamento dei dati nei database [Amazon Relational Database Service \(Amazon RDS\)](#), consulta [Enabling data classification for Amazon RDS database with Macie](#) (Abilitazione della classificazione dei dati per il database Amazon RDS con Macie).

Rilevare i dati sensibili all'interno di DynamoDB:

- [Detecting sensitive data in DynamoDB with Macie](#) (Rilevare i dati sensibili in DynamoDB con Macie) spiega come utilizzare Amazon Macie per rilevare i dati sensibili nelle tabelle [Amazon DynamoDB](#) esportando i dati in Amazon S3 per la scansione.

Soluzioni dei partner AWS:

- Considera la possibilità di utilizzare la nostra ampia rete di partner AWS Partner Network. I partner AWS dispongono di ampi strumenti e framework di conformità che si integrano direttamente con i servizi AWS. I partner possono fornirti una soluzione di governance e conformità su misura per aiutarti a soddisfare le esigenze organizzative.
- Per soluzioni personalizzate nella classificazione dei dati, consulta [Data governance in the age of regulation and compliance requirements](#) (La governance dei dati nell'era delle normative e dei requisiti di conformità).

Gli standard di applicazione di tag adottati dall'organizzazione possono essere applicati automaticamente mediante la creazione e l'implementazione di policy con l'aiuto di AWS Organizations. Le policy sui tag consentono di specificare le regole che definiscono i nomi validi delle chiavi e i valori validi per ciascuna chiave. Puoi scegliere di effettuare solo il monitoraggio, il che ti offre l'opportunità di valutare e ripulire i tag esistenti. Una volta che i tag sono conformi agli standard scelti, puoi attivare l'applicazione nelle policy sui tag per impedire la creazione di tag non conformi. Per maggiori dettagli, consulta [Securing resource tags used for authorization using a service control policy in AWS Organizations](#) (Proteggere i tag delle risorse utilizzati per l'autorizzazione mediante una policy di controllo dei servizi in AWS Organizations) e la policy di esempio su [come prevenire la modifica dei tag da parte di principali non autorizzati](#).

- Per iniziare utilizzando le policy sui tag in [AWS Organizations](#), è fortemente consigliabile seguire il flusso di lavoro descritto in [Nozioni di base sulle policy di tag](#) prima di passare a policy sui tag più avanzate. La comprensione degli effetti dell'applicazione di una semplice policy sui tag a un singolo account prima di estenderla a un'intera unità organizzativa (OU) o organizzazione consente di vedere gli effetti di una policy sui tag prima di applicare la conformità alla policy stessa. [Nozioni di base sulle policy di tag](#) fornisce link a istruzioni per attività più avanzate relative alle policy.
- Considera di valutare altri [servizi e funzionalità di AWS](#) che supportino la classificazione dei dati, che sono elencati nel whitepaper [Data Classification](#) (Classificazione dei dati).

Risorse

Documenti correlati:

- [Getting Started with Amazon Macie](#) (Nozioni di base)
- [Automated data discovery with Amazon Macie](#) (Ricerca automatica di dati con Amazon Macie)

- [Getting started with tag policies](#) (Nozioni di base sulle policy di tag)
- [Detecting PII entities](#) (Rilevamento di entità PII)

Blog correlati:

- [How to use Amazon Macie to preview sensitive data in S3 buckets](#) (Come utilizzare Amazon Macie per visualizzare in anteprima i dati sensibili nei bucket S3).
- [Performing automated sensitive data discovery with Amazon Macie](#). (Esecuzione del rilevamento automatizzato di dati sensibili con Amazon Macie).
- [Common techniques to detect PHI and PII data using AWS Services](#) (Rilevamento e correzione di PII con Amazon AWS)
- [Detecting and redacting PII using Amazon Comprehend](#) (Rilevamento e correzione delle PII con Amazon Comprehend)
- [Securing resource tags used for authorization using a service control policy in AWS Organizations](#) (Protezione dei tag delle risorse utilizzati per l'autorizzazione tramite una policy di controllo dei servizi in AWS Organizations)
- [Enabling data classification for Amazon RDS database with Macie](#) (Consentire la classificazione dei dati per il database Amazon RDS con Macie)
- [Detecting sensitive data in DynamoDB with Macie](#) (Rilevamento di dati sensibili in DynamoDB con Macie)
-

Video correlati:

- [Event-driven data security using Amazon Macie](#) (Sicurezza dei dati guidata dagli eventi con Amazon Macie)
- [Amazon Macie for data protection and governance](#) (Amazon Macie per la protezione e la governance dei dati)
- [Fine-tune sensitive data findings with allow lists](#) (Perfezionare i risultati dei dati sensibili con gli elenchi di permessi)

SEC07-BP02 Definizione dei controlli di protezione dei dati

Proteggi i dati in base al livello di classificazione. Ad esempio, puoi mettere in sicurezza le informazioni classificate come pubbliche utilizzando raccomandazioni pertinenti e allo stesso tempo proteggere i dati sensibili con controlli aggiuntivi.

Utilizzando tag di risorse, account AWS separati per livelli di sensibilità (e potenzialmente anche per avvertimento/enclave/community di interesse), policy IAM, SCP di AWS Organizations, AWS Key Management Service (AWS KMS) e AWS CloudHSM, puoi definire e implementare le policy per la classificazione e la protezione dei dati tramite la crittografia. Ad esempio, se in un progetto sono presenti bucket S3 che contengono dati estremamente critici o istanze Amazon Elastic Compute Cloud (Amazon EC2) che elaborano dati riservati, essi possono essere contrassegnati con un tag `Project=ABC`. Solo il team ristretto conosce il significato del codice del progetto e rappresenta un modo per utilizzare il controllo degli accessi basato su attributi. Puoi definire i livelli di accesso alle chiavi di crittografia AWS KMS tramite policy e concessioni delle chiavi per garantire che solo i servizi appropriati abbiano accesso ai contenuti sensibili tramite un meccanismo sicuro. Se prendi decisioni in merito alle autorizzazioni in base ai tag, devi assicurarti che le autorizzazioni sui tag siano definite in modo appropriato utilizzando le policy dei tag in AWS Organizations.

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

Guida all'implementazione

- Definizione dello schema di identificazione e classificazione dei dati: l'identificazione e la classificazione dei dati è utile a valutare l'impatto potenziale e il tipo di dati archiviati e a stabilire chi può accedervi.
 - [Documentazione di AWS](#)
- Identificazione dei controlli AWS disponibili: scopri i controlli di sicurezza per i servizi AWS che stai utilizzando o che intendi utilizzare. Molti servizi dispongono di una sezione sulla sicurezza nella documentazione.
 - [Documentazione di AWS](#)
- Identificazione delle risorse di conformità AWS: identifica le risorse che AWS mette a disposizione per facilitare i processi di conformità.
 - <https://aws.amazon.com/compliance/>

Risorse

Documenti correlati:

- [Documentazione di AWS](#)
- [Whitepaper sulla classificazione dei dati](#)
- [Nozioni di base su Amazon Macie](#)
- [Testo mancante](#)

Video correlati:

- [Introducing the New Amazon Macie \(Presentazione del nuovo Amazon Macie\)](#)

SEC07-BP03 Automazione dell'identificazione e della classificazione

automatizzare l'identificazione e la classificazione dei dati può aiutarti a implementare i controlli corretti. L'utilizzo dell'automazione per queste operazioni invece dell'accesso diretto da parte di una persona riduce il rischio di errori umani e di esposizione delle persone. È consigliabile valutare l'utilizzo di uno strumento, ad esempio [Amazon Macie](#), che utilizza il machine learning per rilevare, classificare e proteggere automaticamente i dati sensibili in AWS. Amazon Macie riconosce i dati sensibili, quali informazioni personali di identificazione (PII) o di proprietà intellettuale e fornisce pannelli di controllo e allarmi che offrono visibilità su come viene effettuato l'accesso a tali dati o come vengono spostati.

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

Guida all'implementazione

- Utilizzo di Amazon Simple Storage Service (Amazon S3) Inventory: Amazon S3 Inventory è uno degli strumenti che utilizzabili per eseguire audit e segnalare lo stato di replica e crittografia degli oggetti.
 - [Amazon S3 Inventory](#)
- Considerazione di Amazon Macie: Amazon Macie sfrutta il machine learning per scoprire e classificare automaticamente i dati archiviati in Amazon S3.
 - [Amazon Macie](#)

Risorse

Documenti correlati:

- [Amazon Macie](#)
- [Amazon S3 Inventory](#)
- [Whitepaper sulla classificazione dei dati](#)
- [Nozioni di base su Amazon Macie](#)

Video correlati:

- [Introducing the New Amazon Macie \(Presentazione del nuovo Amazon Macie\)](#)

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

la strategia del ciclo di vita definita deve basarsi sul livello di sensibilità e sui requisiti legali e aziendali. Gli aspetti da considerare includono la durata di conservazione dei dati, i processi di distruzione dei dati, la gestione degli accessi ai dati, la trasformazione dei dati e la condivisione dei dati. Nella scelta di una metodologia di classificazione dei dati, è necessario valutare l'usabilità rispetto all'accesso. Devi inoltre gestire vari livelli di accesso e particolarità per implementare un approccio sicuro e utilizzabile per ogni livello. Utilizza sempre un approccio di difesa avanzata e riduci l'accesso umano ai dati e ai meccanismi per trasformare, eliminare o copiare i dati. Ad esempio, richiedi agli utenti di effettuare l'autenticazione in un'applicazione e fornisci all'applicazione, anziché agli utenti, l'autorizzazione di accesso necessaria per eseguire "operazioni a distanza". Inoltre, assicurati che gli utenti provengano da un percorso di rete sicuro e richiedi l'accesso alle chiavi di decrittografia. Utilizza strumenti, pannelli di controllo e generazione di report automatizzata, per fornire agli utenti informazioni ricavate dai dati piuttosto che concedere loro l'accesso diretto ai dati.

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

Guida all'implementazione

- Identifica i tipi di dati: identifica i tipi di dati che stai archiviando o elaborando nel carico di lavoro. Questi potrebbero consistere in testo, immagini, database binari e così via.

Risorse

Documenti correlati:

- [Whitepaper sulla classificazione dei dati](#)
- [Nozioni di base su Amazon Macie](#)

Video correlati:

- [Introducing the New Amazon Macie](#)

Protezione dei dati inattivi

I dati inattivi 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 inattivi 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 che sta tokenizzando; 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.

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 Amazon CloudWatch Insights, 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 inattivi](#)
- [SEC08-BP03 Automatizzazione della protezione dei dati a riposo](#)
- [SEC08-BP04 Applicazione del controllo degli accessi](#)
- [SEC08-BP05 Utilizzo di meccanismi per tenere le persone a distanza dai dati](#)

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: Un meccanismo di gestione delle chiavi dimensionabile, ripetibile e automatizzato. Il meccanismo dovrebbe fornire la possibilità di applicare l'accesso con il privilegio minimo al materiale relativo alla chiave e offrire il giusto equilibrio tra disponibilità, riservatezza e integrità delle chiavi. L'accesso alle chiavi deve essere monitorato e il materiale relativo alla chiave deve essere ruotato utilizzando un processo automatizzato. Il materiale relativo alla chiave non dovrebbe mai essere accessibile alle identità umane.

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 troppo ampie.

Vantaggi dell'adozione di questa best practice: Attraverso 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.

Un'efficace soluzione 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: alto

Guida all'implementazione

Molti requisiti normativi e best practice includono la crittografia dei dati a riposo come controllo di sicurezza fondamentale. Per garantire la conformità, 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 140-2 di livello 3 per proteggere le chiavi. Non esiste un meccanismo per esportare le chiavi AWS KMS convertendole in testo semplice.

Quando si distribuiscono carichi di lavoro utilizzando una strategia multi-account, una [best practice](#) è quella di mantenere le chiavi AWS KMS nello stesso account del carico di lavoro che le utilizza. In questo modello distribuito, la responsabilità della gestione delle chiavi AWS KMS spetta al team applicativo. In altri casi d'uso, le organizzazioni possono 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 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 delle chiavi](#) e policy IAM. Le policy delle chiavi 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 conto dell'utente. Prenditi del tempo per rivedere le [best practice per il controllo degli accessi alle chiavi AWS KMS](#).

Una best practice è quella di monitorare l'uso delle chiavi di crittografia per rilevare 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. Occorre prestare particolare attenzione al monitoraggio dei principali 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 eliminare le chiavi in AWS KMS sono soggetti a [un periodo di attesa](#), che per impostazione predefinita è di 30 giorni, dando 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, la best practice è utilizzare la [crittografia a busta](#) per proteggere i dati. Il comando [SDK di crittografia AWS](#) è in grado di fornire alle applicazioni primitive crittografiche lato client per implementare la crittografia a busta e integrarle con AWS KMS.

Passaggi dell'implementazione

1. Determina le [opzioni di gestione della chiave appropriate](#) (gestita da AWS o gestita dal cliente).
 - 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 delle chiavi.
 - 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 [di un 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 le 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.
 - [Come i servizi AWS utilizzano AWS KMS](#)
 - Per informazioni dettagliate sulle opzioni di crittografia offerte da un servizio AWS, consulta l'argomento Crittografia a riposo nella guida per l'utente o nella guida per 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.
 - [Nozioni di base: AWS Key Management Service \(AWS KMS\)](#)
 - Consulta le [best practice per il controllo degli accessi alle chiavi AWS KMS](#).
4. Considera AWS Encryption SDK: utilizza l'AWS Encryption SDK con l'integrazione di AWS KMS quando la tua applicazione deve crittografare i dati lato client.

- [AWS Encryption SDK](#)
5. Abilita [IAM Access Analyzer](#) per rivedere e inviare notifiche automaticamente se esistono policy delle chiavi AWS KMS eccessivamente permissive.
 6. Abilita [Security Hub](#) per ricevere notifiche in caso di policy delle chiavi 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.
 - Alcune organizzazioni preferiscono separare l'attività di log di AWS KMS in un percorso separato. Per ulteriori informazioni, consulta la sezione [Log delle chiamate API AWS KMS con CloudTrail](#) della guida per gli sviluppatori AWS KMS.

Risorse

Documenti correlati:

- [AWS Key Management Service](#)
- [Servizi e strumenti di crittografia di AWS](#)
- [Protezione dei dati Amazon S3 tramite la crittografia](#)
- [Envelope encryption](#)
- [Digital sovereignty pledge](#)
- [Demystifying AWS KMS key operations, bring your own key, custom key store, and ciphertext portability](#)
- [Dettagli di crittografia di AWS Key Management Service](#)

Video correlati:

- [Come funziona la crittografia in AWS](#)
- [Securing Your Block Storage on AWS \(Protezione dello storage a blocchi in AWS\).](#)
- [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 inattivi

Per i dati a riposo è necessario applicare la crittografia. La crittografia mantiene la riservatezza dei dati sensibili in caso di accesso non autorizzato o di divulgazione accidentale.

Risultato desiderato: la crittografia dei dati privati a riposo deve essere predefinita. La crittografia aiuta a mantenere la riservatezza dei dati e fornisce un ulteriore livello di protezione contro la divulgazione o esfiltrazione intenzionale o involontaria dei dati. I dati crittografati non possono essere letti o consultati senza che siano stati prima decrittografati. Tutti i dati archiviati in modo non crittografato devono essere inventariati e controllati.

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 alle classificazioni dei dati all'interno dei carichi di lavoro. Questo approccio aiuta a proteggere dall'accesso estremamente permissivo quando si utilizza un'unica chiave di crittografia o un numero molto ridotto di chiavi di crittografia per i dati (consulta [SEC07-BP01 Identificazione dei dati all'interno del carico di lavoro](#)).

AWS Key Management Service (AWS KMS) si integra con molti servizi AWS per semplificare la crittografia dei dati a riposo. Ad esempio, in Amazon Simple Storage Service (Amazon S3), puoi impostare la [crittografia predefinita](#) su un bucket in modo che i nuovi oggetti vengano automaticamente crittografati. 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 sulle chiavi.

Inoltre, [Amazon Elastic Compute Cloud \(Amazon EC2\)](#) e [Amazon S3](#) applicano la crittografia impostandone un tipo predefinito. Puoi servirti della [Regole di AWS Config](#) per verificare automaticamente l'utilizzo della crittografia, ad esempio, per [volumi Amazon Elastic Block Store \(Amazon EBS\)](#), [istanze Amazon Relational Database Service \(Amazon RDS\)](#) e [bucket Amazon S3](#).

AWS offre anche soluzioni per la crittografia lato client, consentendo di crittografare i dati prima di caricarli nel cloud. AWS Encryption SDK offre un metodo per crittografare i dati utilizzando 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. Considera 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 trasparente dei dati (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 Amazon DynamoDB Encryption Client consente inoltre di crittografare e firmare gli elementi prima del caricamento in una tabella DynamoDB.

Passaggi dell'implementazione

- Applicazione della crittografia a riposo per Amazon S3: implementa [la crittografia predefinita del bucket Amazon S3](#).

Configura [la crittografia predefinita per i nuovi volumi Amazon EBS](#): specifica se desideri che tutti i nuovi volumi Amazon EBS vengano creati in forma crittografata, con la possibilità di utilizzare la chiave predefinita fornita da AWS o una chiave creata dall'utente.

Configura Amazon Machine Image (AMI) crittografate: copiando un'AMI esistente con crittografia abilitata verrà eseguita la crittografia automatica di volumi root e delle snapshot.

Configura la [crittografia Amazon RDS](#): configura la crittografia per i cluster di database Amazon RDS e le snapshot a riposo utilizzando l'opzione di crittografia.

Crea e configura le chiavi AWS KMS con policy che limitino l'accesso ai principali appropriati per ogni classificazione di dati: ad esempio, crea una chiave AWS KMS per la crittografia dei dati di produzione e una chiave diversa per la crittografia dei dati di sviluppo o di test. Puoi anche fornire l'accesso alle chiavi ad altri Account AWS. Considera la possibilità di avere 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 per crittografare gli

artefatti di sviluppo per dare all'account di produzione la possibilità di decrittografare tali artefatti. L'ambiente di produzione può quindi importare i dati decrittografati per utilizzarli nella produzione.

Configura la crittografia in altri servizi AWS: per gli altri servizi AWS utilizzati, consulta la [documentazione sulla sicurezza](#) del servizio per individuare le opzioni di crittografia del servizio.

Risorse

Documenti correlati:

- [AWS Crypto Tools](#)
- [Documentazione di AWS](#)
- [AWS Encryption SDK](#)
- [AWS KMS Cryptographic Details Whitepaper](#) (Whitepaper sui dettagli crittografici di AWS KMS)
- [AWS Key Management Service](#)
- [AWS cryptographic services and tools](#) (servizi e strumenti di crittografia AWS)
- [Crittografia Amazon EBS](#)
- [Default encryption for Amazon EBS volumes](#) (Crittografia predefinita per i volumi Amazon EBS)
- [Crittografia delle risorse Amazon RDS](#)
- [How do I enable default encryption for an Amazon S3 bucket?](#) (Come si attiva la crittografia predefinita per un bucket Amazon S3?)
- [Protecting Amazon S3 Data Using Encryption](#) (Protezione dei dati Amazon S3 mediante crittografia)

Video correlati:

- [How Encryption Works in AWS](#) (Come funziona la crittografia in AWS)
- [Securing Your Block Storage on AWS](#) (Protezione dello storage a blocchi in AWS)

SEC08-BP03 Automatizzazione della protezione dei dati a riposo

utilizza strumenti automatizzati per convalidare e applicare la protezione dei dati a riposo in modo continuo; ad esempio verifica che siano presenti solo risorse di storage crittografate. Puoi [automatizzare la convalida della crittografia di tutti i volumi EBS](#) utilizzando [Regole di AWS Config](#). [AWS Security Hub](#) può anche verificare una serie di controlli diversi tramite verifiche

automatiche a fronte di standard di sicurezza. Inoltre, le Regole di AWS Config possono correggere automaticamente [le risorse non conformi](#).

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

Guida all'implementazione

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.

Applica la crittografia dei dati a riposo: devi accertarti che l'unico modo per archiviare i dati sia l'utilizzo della crittografia. AWS KMS si integra perfettamente con molti servizi AWS per semplificare la crittografia di tutti i dati inattivi. Ad esempio, in Amazon Simple Storage Service (Amazon S3) puoi impostare [la crittografia predefinita](#) su un bucket in modo che tutti i nuovi oggetti vengano crittografati automaticamente. Inoltre, [Amazon EC2](#) e [Amazon S3](#) supportano l'applicazione della crittografia impostando la crittografia predefinita. Puoi utilizzare [AWS Managed Config Rules](#) per verificare automaticamente che stai utilizzando la crittografia, ad esempio, per i [volumi EBS](#), [le istanze Amazon Relational Database Service \(Amazon RDS\)](#) e [bucket Amazon S3](#).

Risorse

Documenti correlati:

- [AWS Crypto Tools](#)
- [SDK di crittografia AWS](#)

Video correlati:

- [How Encryption Works in AWS \(Come funziona la crittografia in AWS\)](#)
- [Securing Your Block Storage on AWS](#)

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, quindi applica il principio del privilegio minimo. Impedisce l'accesso pubblico ai dati.

Risultato desiderato: verifica che solo gli utenti autorizzati possano accedere ai dati in base al principio "Need-to-Know" (necessità di sapere). La protezione dei dati è assicurata da backup regolari e dal controllo delle versioni, per evitare che i dati vengano modificati o eliminati intenzionalmente o inavvertitamente. 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: basso

Guida all'implementazione

La protezione dei dati a riposo può essere garantita da diversi controlli, tra cui l'accesso (utilizzando il privilegio minimo), l'isolamento e il controllo delle versioni. L'accesso ai dati deve essere soggetto a audit mediante meccanismi di rilevazione, come AWS CloudTrail e log sul livello di servizio, come i log di accesso di Amazon Simple Storage Service (Amazon S3). Per ridurre nel tempo la quantità di dati disponibili pubblicamente, è necessario fare un inventario dei dati accessibili pubblicamente e creare un piano.

Amazon S3 Glacier Vault Lock e Amazon S3 Object Lock forniscono un controllo di accesso obbligatorio per gli oggetti in Amazon S3: una volta bloccata con l'opzione di conformità, una policy Vault non può essere modificata nemmeno dall'utente root fino alla scadenza del blocco.

Passaggi dell'implementazione

- Applica il controllo degli accessi: applica il controllo degli accessi con privilegio minimo, incluso l'accesso alle chiavi di crittografia.
- Separa i dati in base a diversi livelli di classificazione: utilizza diversi Account AWS per i livelli di classificazione dei dati e gestisci tali account utilizzando [AWS Organizations](#).
- Rivedi le policy di AWS Key Management Service (AWS KMS): [rivedi il livello di accesso](#) concesso nelle policy di AWS KMS.

- Rivedi le autorizzazioni dei bucket e degli oggetti di Amazon S3: rivedi regolarmente il livello di accesso concesso nelle policy dei bucket S3. La best practice è evitare di utilizzare bucket leggibili o scrivibili pubblicamente. Valuta l'utilizzo di [AWS Config](#) per rilevare i bucket disponibili pubblicamente e di Amazon CloudFront per fornire contenuti provenienti da Amazon S3. Verifica che i bucket che non consentono l'accesso pubblico siano configurati correttamente per impedirlo. Per impostazione predefinita, tutti i bucket S3 sono privati e possono accedervi soltanto gli utenti a cui è stato esplicitamente accordato l'accesso.
- Abilita [AWS IAM Access Analyzer](#): IAM Access Analyzer analizza i bucket Amazon S3 e genera un risultato quando [una policy S3 concede l'accesso a un'entità esterna](#).
- Abilita il [controllo delle versioni Amazon S3](#) e del [blocco degli oggetti](#) laddove appropriato.
- Utilizza [Amazon S3 Inventory](#): Amazon S3 Inventory può essere utilizzato per effettuare audit e report sullo stato di replica e crittografia degli oggetti S3.
- Rivedi le autorizzazioni di [condivisione Amazon EBS](#) e [AMI](#): le autorizzazioni di condivisione possono consentire la condivisione di immagini e volumi con Account AWS esterni al carico di lavoro.
- Rivedi periodicamente le condivisioni di [AWS Resource Access Manager](#) per stabilire se le risorse devono continuare ad essere condivise. Resource Access Manager consente di condividere risorse, come le policy del firewall di rete AWS, le regole del resolver Amazon Route 53 e le sottoreti, all'interno dei Amazon VPC. Sottoponi regolarmente a 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](#) (Whitepaper sui dettagli crittografici di AWS KMS)
- [Introduction to Managing Access Permissions to Your Amazon S3 Resources](#) (Introduzione alla gestione delle autorizzazioni di accesso alle risorse di Amazon S3)
- [Overview of managing access to your AWS KMS resources](#) (Panoramica della gestione dell'accesso alle risorse AWS KMS)

- [Regole di AWS Config](#) (Regole AWS Config)
- [Amazon S3 + Amazon CloudFront: A Match Made in the Cloud](#) (Amazon S3 + Amazon CloudFront: un abbinamento perfetto nel cloud)
- [Utilizzo del controllo delle versioni](#)
- [Utilizzo del blocco oggetti Amazon S3](#)
- [Condivisione di uno snapshot Amazon EBS](#)
- [AMI condivise](#)
- [Hosting a single-page application on Amazon S3](#) (Ospitare un'applicazione a pagina singola su Amazon S3)

Video correlati:

- [Securing Your Block Storage on AWS](#) (Protezione dello storage a blocchi in AWS)

SEC08-BP05 Utilizzo di meccanismi per tenere le persone a distanza dai dati

Evita a tutti gli utenti di accedere direttamente a dati e sistemi sensibili in circostanze operative normali. Ad esempio, usa un flusso di lavoro per la gestione delle modifiche per gestire le istanze Amazon Elastic Compute Cloud (Amazon EC2) tramite strumenti, invece di consentire l'accesso diretto o tramite un host bastione. A tal fine puoi utilizzare [AWS Systems Manager Automation](#), che utilizza [documenti di automazione](#) che contengono le fasi utilizzate per eseguire le attività. Questi documenti possono essere archiviati nel controllo sorgente, revisionati in peering prima dell'esecuzione e testati accuratamente per ridurre al minimo i rischi rispetto all'accesso alla shell. Gli utenti aziendali possono utilizzare un pannello di controllo anziché accedere direttamente a un datastore per eseguire query. Se non vengono utilizzate le pipeline CI/CD, determina quali controlli e processi sono necessari per fornire in modo adeguato un meccanismo di accesso di tipo break-glass normalmente disabilitato.

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

Guida all'implementazione

- Implementazione di meccanismi per tenere le persone lontane dai dati: i meccanismi includono l'utilizzo di pannelli di controllo, ad esempio Amazon QuickSight, per mostrare i dati agli utenti anziché eseguire query direttamente.

- [Amazon QuickSight](#)
- Automazione della gestione della configurazione: esegui azioni a distanza, applica e convalida in automatico configurazioni sicure sfruttando un apposito servizio o strumento di gestione. Evita l'uso di bastion host o l'accesso diretto alle istanze EC2.
- [AWS Systems Manager](#)
- [AWS CloudFormation](#)
- [Pipeline CI/CD per modelli AWS CloudFormation su AWS](#)

Risorse

Documenti correlati:

- [Whitepaper per i dettagli della crittografia di AWS KMS](#)

Video correlati:

- [Come funziona la crittografia in AWS](#)
- [Securing Your Block Storage on AWS \(Protezione dello storage a blocchi in AWS\).](#)

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 e sedi on-premise: Puoi utilizzare [AWS PrivateLink](#) per creare una connessione di rete sicura e privata tra Amazon Virtual Private Cloud (Amazon VPC) oppure una connettività on-premise ai 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 instradamento. 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 Automatizzazione del rilevamento degli accessi indesiderati ai dati](#)
- [SEC09-BP04 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 automaticamente 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: alto

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 l'attrito associato alla loro gestione.

AWS fornisce due servizi per gestire i certificati PKI generici: [AWS Certificate Manager](#) e [AWS Private Certificate Authority \(AWS Private CA\)](#). ACM è il servizio principale utilizzato dai clienti per fornire, gestire e implementare certificati da utilizzare sia in carichi di lavoro di AWS pubblici che privati. ACM emette certificati utilizzando AWS Private CA e [si integra](#) con molti altri servizi AWS gestiti per fornire certificati TLS sicuri per i carichi di lavoro.

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 fiducia sul lato client della connessione TLS. Oltre ai casi d'uso TLS, AWS Private CA può essere utilizzato per 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 utilizzare la strategia di [IAM Roles Anywhere](#) per fornire credenziali temporanee IAM ai carichi di lavoro on-premise 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 fornisce meccanismi specializzati per [l'onboarding di dispositivi IoT](#) nella tua infrastruttura a chiave pubblica su larga scala.

Considerazioni sulla creazione di una gerarchia CA privata

Quando è necessario stabilire una CA privata, è importante prestare particolare attenzione a progettare correttamente la gerarchia della CA fin dall'inizio. Quando si crea una gerarchia CA privata è consigliabile distribuire ogni 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 deve essere utilizzata solo per emettere 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 [Pianificazione dell'implementazione di AWS Private CA](#).

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 può essere utilizzato per implementare certificati TLS per server Web, sistemi di bilanciamento del carico o altri usi per certificati pubblicamente affidabili.
- Considera il servizio [AWS Private CA](#) quando è necessario stabilire una gerarchia di autorità di certificazione privata o accedere a certificati esportabili. ACM può quindi essere utilizzato per emettere [molti tipi di certificati dell'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](#).

2. Implementa il rinnovo automatico dei certificati quando possibile:

- utilizza [rinnovo gestito di ACM](#) per i certificati emessi da ACM insieme ai servizi AWS gestiti integrati.

3. Stabilisci percorsi di registrazione e controllo:

- Abilita [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.
- Genera e rivedi periodicamente [rapporti di audit](#) che elencano i certificati che la tua CA privata ha emesso o revocato. 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 [Pianificazione di un elenco di revoche di certificati \(CRL\)](#).

Risorse

Best practice correlate:

- [SEC02-BP02 Utilizzo di credenziali temporanee](#)
- [SEC08-BP01 Implementazione della gestione sicura delle chiavi](#)
- [SEC09-BP04 Autenticazione delle comunicazioni di rete](#)

Documenti correlati:

- [Come ospitare e gestire un'intera infrastruttura di certificati privata 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](#)
- [Workshop sulla gestione dei dispositivi IOT](#) (incluso 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: tutti i dati devono essere crittografati in transito utilizzando protocolli e suite di crittografia TLS sicuri. Il traffico di rete tra le tue risorse e Internet deve essere crittografato per evitare l'accesso non autorizzato ai dati. Il traffico di rete esclusivamente all'interno dell'ambiente AWS deve essere crittografato utilizzando TLS, ove possibile. La rete interna di AWS è crittografata per impostazione predefinita e il traffico di rete all'interno di un VPC non può essere sottoposto a spoofing o sniffing, a meno che una parte non autorizzata non abbia ottenuto l'accesso alla risorsa che sta generando il traffico (come le istanze Amazon EC2 e i container Amazon ECS). Considera la possibilità di proteggere il traffico da rete a rete con una rete privata virtuale (VPN) IPsec.

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 forniscono crittografia in transito quando comunicano con le API AWS. I protocolli non sicuri, come HTTP, possono essere sottoposti a audit e bloccati in un VPC tramite l'uso di gruppi di sicurezza. Le richieste HTTP possono essere [reindirizzate automaticamente a HTTPS](#) in Amazon CloudFront o su un [Application Load Balancer](#). 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 facilitare la crittografia del traffico. Verifica che i tuoi client effettuino chiamate alle API AWS utilizzando almeno TLS 1.2, poiché [AWS considererà obsoleto l'utilizzo di TLS 1.0 e 1.1 da giugno 2023](#). Per requisiti particolari, in Marketplace AWS sono disponibili soluzioni di terze parti.

Passaggi dell'implementazione

- Applicazione della crittografia in transito: i requisiti di crittografia definiti devono 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 i protocolli sicuri nei servizi edge: [configura HTTPS con Amazon CloudFront](#) e utilizza un [profilo di sicurezza appropriato per la postura di sicurezza e il caso d'uso](#).
- Utilizza 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 sistemi di bilanciamento del carico: seleziona una policy di sicurezza che fornisca le suite di crittografia più efficaci supportate dai client che si conatteranno all'ascoltatore. [Configurazione di un ascoltatore HTTPS per Application Load Balancer](#).
- Configura protocolli sicuri in Amazon Redshift: configura il cluster per richiedere una [connessione Secure Socket Layer \(SSL\) o Transport Layer Security \(TLS\)](#).
- Configura protocolli sicuri: analizza la documentazione relativa al servizio AWS per determinare le capacità di crittografia in transito.
- Configura l'accesso sicuro durante il caricamento di bucket Amazon S3: utilizza i controlli delle policy del bucket Amazon S3 per [applicare l'accesso sicuro](#) ai dati.
- Valuta l'utilizzo di [AWS Certificate Manager](#): ACM consente di fornire, gestire e implementare certificati TLS pubblici da utilizzare con i servizi AWS.
- Valuta l'utilizzo di [AWS Private Certificate Authority](#) per esigenze di PKI private: AWS Private CA consente di creare gerarchie di autorità di certificazione (CA) private per emettere certificati X.509 end-entity che possono essere usati per creare canali TLS crittografati.

Risorse

Documenti correlati:

- [Documentazione di AWS](#)
- [Utilizzo di HTTPS con CloudFront](#)
- [Connetti il tuo VPC a reti remote utilizzando AWS Virtual Private Network](#)
- [Configurazione di un ascoltatore HTTPS per Application Load Balancer](#)
- [Tutorial: configurazione di SSL/TLS su Amazon Linux 2 Amazon Linux 2](#)
- [Utilizzo di SSL/TLS per crittografare una connessione a un'istanza database](#)
- [Configurazione delle opzioni di sicurezza per le connessioni](#)

SEC09-BP03 Automatizzazione del rilevamento degli accessi indesiderati ai dati

Usa strumenti come Amazon GuardDuty per rilevare in automatico attività o tentativi sospetti di trasferire i dati al di fuori di limiti predefiniti. Ad esempio, GuardDuty può rilevare attività di lettura di Amazon Simple Storage Service (Amazon S3) inusuale con [Exfiltration:S3/AnomalousBehavior finding](#). Oltre a GuardDuty, si possono utilizzare i [Registri di flusso Amazon VPC](#), che acquisiscono informazioni sul traffico di rete, con Amazon EventBridge per attivare il rilevamento di connessioni anomale, riuscite e negate. [Amazon S3 Access Analyzer](#) aiuta a valutare quali dati sono accessibili a chi nei bucket Amazon S3.

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

Guida all'implementazione

- Automazione del rilevamento di accessi ai dati non intenzionali: utilizza uno strumento o un meccanismo di rilevamento per rilevare automaticamente i tentativi di spostamento dei dati all'esterno dei confini definiti, ad esempio, per individuare un sistema di database che copia i dati su un host sconosciuto.
 - [Log di flusso VPC](#)
- Valutazione di Amazon Macie: Amazon Macie è un servizio di sicurezza e privacy dei dati completamente gestito che utilizza il machine learning e il pattern matching per rilevare e proteggere i dati sensibili all'interno di AWS.
 - [Amazon Macie](#)

Risorse

Documenti correlati:

- [Log di flusso VPC](#)
- [Amazon Macie](#)

SEC09-BP04 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 l'autenticazione e l'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 flussi di traffico del piano dati e del piano di controllo (control-plane) ben definiti 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 più elevato di sicurezza affinché le azioni vengano eseguite solo da entità autenticate.
- Migliora il disaccoppiamento dei servizi definendo e applicando chiaramente le interfacce di trasferimento dei dati previste.
- Migliora il monitoraggio, la registrazione in log e la risposta agli incidenti tramite l'attribuzione delle richieste e interfacce di comunicazione ben definite.
- Fornisce un livello elevatissimo di difesa ai carichi di lavoro combinando i controlli di rete con i controlli di autenticazione e autorizzazione.

Livello di rischio associato alla mancata adozione di questa best practice: basso

Guida all'implementazione

I modelli di traffico di rete del carico di lavoro possono essere suddivisi in due categorie:

- Il traffico orizzontale (sinistra-destra) rappresenta i flussi di traffico tra servizi che costituiscono un carico di lavoro.
- Il traffico verticale (alto-basso) rappresenta i flussi di traffico tra il carico di lavoro e i consumatori.

Mentre crittografare il traffico verticale (alto-basso) è prassi comune, proteggere il traffico orizzontale (sinistra-destra) 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 [AWS Signature Version 4 \(SigV4\)](#) per autenticare il chiamante, indipendentemente dalla rete da cui proviene la richiesta. Questa autenticazione garantisce che le API 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 [Amazon API Gateway](#) consentono di utilizzare lo stesso protocollo di firma SigV4 per aggiungere funzionalità di autenticazione e autorizzazione al traffico orizzontale (sinistra-destra) ai carichi di lavoro. Se le risorse esterne all'ambiente AWS devono comunicare con servizi che richiedono l'autenticazione e l'autorizzazione basate su SigV4, è possibile utilizzare [AWS Identity and Access Management \(IAM\) Roles Anywhere](#) sulla risorsa 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 orizzontale (sinistra-destra) 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 Private Certificate Authority (AWS Private CA). È possibile utilizzare servizi come [Amazon API Gateway](#) e [AWS App Mesh](#) per fornire l'autenticazione mTLS per la comunicazione tra carichi di lavoro a tutti i livelli. 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 generalmente utilizzati per controllare l'accesso ai servizi da parte degli utenti, ma stanno diventando popolari anche per il traffico a livello di servizi. API Gateway fornisce un [sistema di autorizzazione JSON Web Token \(JWT\)](#), che consente ai carichi di lavoro di limitare l'accesso alle route API utilizzando JWT emessi da gestori dell'identità digitale OIDC o OAuth 2.0. Gli ambiti OAuth2 possono essere utilizzati come base

per decisioni di autorizzazione essenziali, ma i controlli di autorizzazione devono comunque essere 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 di alto profilo è definire i flussi di traffico del carico di lavoro.
- Crea un diagramma del flusso di dati che definisca chiaramente come vengono trasmessi i 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 dei dati rifletta accuratamente il comportamento del carico di lavoro in fase di esecuzione.
- Un diagramma del flusso dei dati può essere utile anche quando si esegue un esercizio di modellazione delle minacce, come descritto in [SEC01-BP07 Identificare le minacce e dare priorità alle mitigazioni utilizzando un modello di minaccia](#).
- Definisci i controlli di rete: considera le funzionalità AWS per stabilire controlli di rete allineati ai flussi di dati. Sebbene i confini della rete non debbano costituire l'unico elemento di controllo della sicurezza, essi 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 risorse.
 - Valuta l'utilizzo di [AWS PrivateLink](#) per comunicare sia con AWS che con i servizi 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 l'autenticazione e l'autorizzazione tra i servizi del carico di lavoro: scegli il set di servizi AWS più appropriato per fornire flussi di traffico autenticati e crittografati nel carico di lavoro.
 - Valuta l'ipotesi di utilizzare [Amazon VPC Lattice](#) per la sicurezza della comunicazione tra servizi. VPC Lattice può utilizzare l'[autenticazione SigV4 combinata con le policy di autenticazione](#) per controllare l'accesso a livello di servizi.
 - Per la comunicazione tra servizi tramite mTLS, valuta l'ipotesi di utilizzare [API Gateway](#) o [App Mesh](#). [AWS Private CA](#) può essere utilizzato per stabilire una gerarchia di autorità di certificazione (CA) private in grado di emettere certificati da utilizzare con mTLS.
 - Quando esegui l'integrazione con servizi che utilizzano OAuth 2.0 o OIDC, considera [l'utilizzo del sistema di autorizzazione JWT da parte di API Gateway](#).

- Per la comunicazione tra il carico di lavoro e i dispositivi IoT, considera l'utilizzo di [AWS IoT Core](#), che offre diverse opzioni per la crittografia e l'autenticazione del traffico di rete.
- Monitora gli accessi non autorizzati: monitora continuamente i canali di comunicazione non intenzionali, i responsabili non autorizzati che tentano di accedere alle risorse protette e altri schemi di accesso impropri.
- In caso di utilizzo di VPC Lattice per gestire l'accesso ai servizi, valuta la possibilità di abilitare e monitorare i [log di accesso di 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.
- Valuta la possibilità di abilitare i [log di flusso VPC](#) per acquisire i metadati sui flussi di rete e verificare periodicamente la presenza di anomalie.
- Consulta il manuale [AWS Security Incident Response Guide](#) e la [sezione relativa alle risposte agli incidenti](#) del Pilastro di sicurezza del Framework AWS Well-Architected per ulteriori indicazioni su pianificazione, simulazione e risposte agli incidenti di sicurezza.

Risorse

Best practice correlate:

- [SEC03-BP07 Analisi dell'accesso pubblico e multi-account](#)
- [SEC02-BP02 Utilizzo di credenziali temporanee](#)
- [SEC01-BP07 Identificare le minacce e dare priorità alle mitigazioni utilizzando un modello di minaccia.](#)

Documenti correlati:

- [Valutazione dei metodi di controllo degli accessi per proteggere le API Amazon API Gateway](#)
- [Configurazione dell'autenticazione TLS reciproca per una REST API](#)
- [Come proteggere gli endpoint HTTP API Gateway con il sistema di autorizzazione JWT](#)
- [Autorizzazione delle chiamate dirette ai servizi AWS mediante il provider di credenziali AWS IoT Core](#)
- [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:

- [Workshop Amazon VPC Lattice](#)
- [Zero-Trust Episode 1 – The Phantom Service Perimeter workshop](#)

Risposta agli imprevisti

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](#)
- [Progettazione degli obiettivi di risposta al cloud](#)
- [Preparazione](#)
- [Operazioni](#)
- [Attività post-incidente](#)

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. I fondamenti di un programma di risposta agli incidenti nel cloud efficace sono Preparazione, Operazione e 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 gli stakeholder, 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 modelli di risposta all'interno del cloud, dove si verificano l'evento e i dati.

- Individuazione dei dati esistenti e di quelli necessari: 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 redistribuzione: se un'anomalia di sicurezza può essere attribuita a una configurazione errata, la correzione potrebbe consistere semplicemente nella rimozione della varianza implementando nuovamente 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.
- Automazione 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.
- Scelta di soluzioni dimensionabili: cerca di associare la scalabilità dell'approccio aziendale al cloud computing. Implementa meccanismi di rilevamento e risposta dimensionabili nei tuoi ambienti per ridurre efficacemente il tempo che intercorre tra rilevamento e risposta.
- Individuazione delle lacune e miglioramento del processo: 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.
- **Elaborazione:** 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 ambiti 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 Distribuzione 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 che potrebbero aiutare l'organizzazione a rispondere a un incidente.

Quando definisci come affrontare la risposta agli incidenti nel cloud, insieme ad altri team (ad esempio il consulente legale, la leadership dell'organizzazione, le parti interessate, i servizi AWS Support e altri), devi identificare il personale chiave, le parti interessate e i contatti pertinenti. Per ridurre le dipendenze e i tempi di risposta, assicurati che il personale, i team di sicurezza specializzati e i team che rispondono agli incidenti ricevano informazioni sui servizi che utilizzi e abbiano l'opportunità di esercitarsi direttamente.

Ti invitiamo a identificare i partner di sicurezza AWS esterni in grado di fornirti competenze e una prospettiva diversa per potenziare le tue capacità di risposta. I partner di sicurezza affidabili possono aiutarti a identificare potenziali rischi o minacce che potresti non conoscere.

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

Guida all'implementazione

- Identificazione del personale chiave all'interno dell'organizzazione: Conserva un elenco di contatti del personale interno alla tua organizzazione che potrebbe essere necessario coinvolgere per rispondere a un incidente ed effettuare il ripristino.
- Identificazione dei partner esterni: Se necessario, coinvolgi partner esterni che possano aiutarti a rispondere a un incidente e a effettuare il ripristino.

Risorse

Documenti correlati:

- [AWS Incident Response Guide \(Guida alle risposte agli incidenti\)](#)

Video correlati:

- [Prepare for and respond to security incidents in your AWS environment](#)

Esempi correlati:

SEC10-BP02 Sviluppo di piani di gestione degli incidenti

Il primo documento da sviluppare 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 chiaramente definiti 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 ti aiuteranno a rispondere in modo tempestivo. Potrebbero essere già presenti processi di risposta agli incidenti. Indipendentemente dallo stato attuale, è importante aggiornare, iterare e testare regolarmente i processi di risposta agli incidenti.

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

Guida all'implementazione

Un piano di gestione degli incidenti è fondamentale per rispondere, mitigare e ripristinare lo stato a seguito del potenziale impatto degli incidenti di sicurezza. Un piano di gestione degli incidenti è un processo strutturato per identificare, correggere e rispondere tempestivamente agli incidenti di sicurezza.

Il cloud ha molti degli stessi ruoli e requisiti operativi che si trovano in un ambiente on-premise. Quando si crea un piano di gestione degli incidenti è importante tenere conto delle strategie di risposta e ripristino che meglio si allineano ai risultati aziendali e ai requisiti di conformità. Ad esempio, se gestisci carichi di lavoro in AWS conformi a FedRAMP negli Stati Uniti, è utile attenersi a [NIST SP 800-61 Computer Security Handling Guide \(NIST SP 800-61 Guida alla gestione della sicurezza informatica\)](#). Analogamente, quando gestisci carichi di lavoro con informazioni di identificazione personale (PII) europee, considera ad esempio come potresti proteggere e rispondere a problemi relativi alla residenza dei dati come richiesto dalle [normative del Regolamento generale sulla protezione dei dati \(GDPR\) dell'Unione europea](#).

Quando crei un piano di gestione degli incidenti per i carichi di lavoro in AWS, inizia con il [modello di responsabilità condivisa AWS](#) per creare un approccio di difesa in profondità in 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 \(Guida alle risposte agli incidenti di sicurezza di AWS\)](#) illustra i concetti chiave e le linee guida di base per la creazione di un piano di gestione degli incidenti incentrato sul cloud.

Un piano di gestione degli incidenti efficace deve essere continuamente iterato per rimanere in linea con l'obiettivo delle operazioni cloud. Prendi in considerazione l'utilizzo dei piani di implementazione descritti di seguito durante la creazione e l'evoluzione del tuo piano di gestione degli incidenti.

Passaggi dell'implementazione

Definizione di ruoli e responsabilità

La gestione degli eventi di sicurezza richiede disciplina interorganizzativa e propensione all'azione. All'interno della struttura organizzativa, dovrebbero esserci molte persone da considerarsi responsabili, affidabili, consultabili o informate durante un incidente, come i rappresentanti delle risorse umane (HR), i membri del team esecutivo e quelli dell'ufficio legale. Considera questi ruoli e queste responsabilità e se è necessario coinvolgere terze parti. Si noti che molte aree geografiche

hanno leggi locali che regolano cosa dovrebbe e non dovrebbe essere fatto. Sebbene possa sembrare burocratico creare una tabella delle persone responsabili, affidabili, consultabili e informate (RACI) per i piani di risposta relativi alla sicurezza, ciò facilita una comunicazione rapida e diretta e delinea chiaramente la leadership nelle diverse fasi dell'evento.

Durante un incidente, includere i proprietari e gli sviluppatori delle applicazioni e delle risorse interessate è fondamentale perché sono esperti in materia (PMI) che possono fornire informazioni e contesto per aiutare a valutare l'impatto. Assicurati di fare pratica e instaurare relazioni con gli sviluppatori e i proprietari delle applicazioni prima di affidarti alla loro esperienza per la gestione della risposta agli incidenti. I proprietari di applicazioni o le PMI, come gli amministratori o gli ingegneri del cloud, potrebbero dover intervenire in situazioni in cui l'ambiente non è noto oppure è complesso o chi risponde non ha accesso all'ambiente interessato.

Infine, nell'indagine o nella risposta potrebbero essere coinvolti partner affidabili perché possono fornire competenze aggiuntive e capacità analitiche strategiche. Quando non disponi di queste competenze nel tuo team, potresti voler assumere una persona esterna per assistenza.

Analisi del team di risposta di AWS e del supporto

- AWS Support
 - [AWS Support](#) offre un'ampia gamma di piani che forniscono accesso agli strumenti e alla competenza che genera successo e stato operativo delle soluzioni AWS. Se hai bisogno di supporto tecnico e di 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.
 - Valuta l'ipotesi di utilizzare il [Centro di supporto](#) in AWS Management Console (è richiesto l'accesso) come punto di contatto centralizzato per ottenere assistenza per problemi che riguardano le tue risorse AWS. L'accesso a AWS Support è controllato da AWS Identity and Access Management. Per ulteriori informazioni sull'accesso alle funzionalità AWS Support, consulta la sezione [Nozioni di base su AWS Support](#).
- Team di risposta agli incidenti dei clienti AWS (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 AWS](#).
 - Quando il team AWS CIRT ti supporta, fornisce assistenza nella valutazione e nel ripristino di un evento di sicurezza attivo AWS. Può aiutare nell'analisi delle cause principali con l'uso dei log dei servizi AWS e fornire suggerimenti per il ripristino. Può anche fornire consigli e best practice sulla sicurezza per aiutarti a evitare eventi di sicurezza in futuro.

- I clienti AWS possono coinvolgere il team AWS CIRT attraverso un [caso AWS Support](#).
- Supporto per la risposta agli attacchi DDoS
 - AWS offre [AWS Shield](#), che fornisce un servizio di protezione DDoS (Distributed Denial of Service) gestito che protegge le applicazioni Web in esecuzione su AWS. Shield fornisce un rilevamento sempre attivo e mitigazioni automatiche in linea che possono ridurre al minimo i tempi di inattività e la latenza delle applicazioni, quindi non è necessario utilizzare AWS Support per avvalersi della protezione dagli attacchi DDoS. Esistono due livelli di Shield: AWS Shield Standard e AWS Shield Advanced. Per maggiori informazioni sulle differenze tra questi due livelli, consulta la [documentazione delle funzionalità di Shield](#).
- AWS Managed Services (AMS)
 - [AWS Managed Services \(AMS\)](#) offre gestione continua dell'infrastruttura AWS, così potrai occuparti a tempo pieno delle tue applicazioni. Grazie all'implementazione delle best practice per la gestione dell'infrastruttura, AMS riduce il sovraccarico operativo e il livello di rischio. 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. Quando viene avviato un avviso, AMS segue 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 gli obiettivi e le funzioni del team di risposta agli incidenti.
- Ruoli e responsabilità: elenca le parti interessate alla risposta agli incidenti e descrive in dettaglio i loro ruoli quando si verifica un incidente.
- Un piano di comunicazione: dettagli sulle informazioni di contatto e su come comunichi 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:** enumera 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 prioritizzazione degli incidenti:** descrive in dettaglio come classificare la gravità di un incidente, come assegnare la priorità all'incidente e, quindi, in che modo le definizioni di gravità influiscono sulle procedure di escalation.

Sebbene queste sezioni siano comuni a società 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:

- [SEC 4 \(In che modo individui ed esami gli eventi di sicurezza?\)](#)

Documenti correlati:

- [AWS Security Incident Response Guide \(Guida alle risposte agli incidenti di sicurezza di AWS\)](#)
- [NIST: Guida alla gestione degli incidenti di sicurezza informatica](#)

SEC10-BP03 Preparazione di funzionalità forensi

Prima che si verifichi un incidente di sicurezza, puoi sviluppare le 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-premise 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 l'ambiente e la struttura di Account AWS per le funzionalità forensi, definisci le tecnologie necessarie in modo da eseguire efficacemente le metodologie forensi in quattro fasi:

- **Raccolta:** acquisisci 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:** studia i dati raccolti per comprendere l'incidente e trarre le conclusioni.
- **Segnalazione:** 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 governare centralmente un ambiente AWS mentre le risorse AWS crescono e si dimensionano. Un'organizzazione AWS consolida gli Account AWS in modo da poterli amministrare come una singola unità. È possibile utilizzare le unità organizzative 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 una Unità organizzativa di sicurezza e una Unità organizzativa forense. All'interno dell'unità organizzativa di sicurezza, è necessario disporre degli account per:

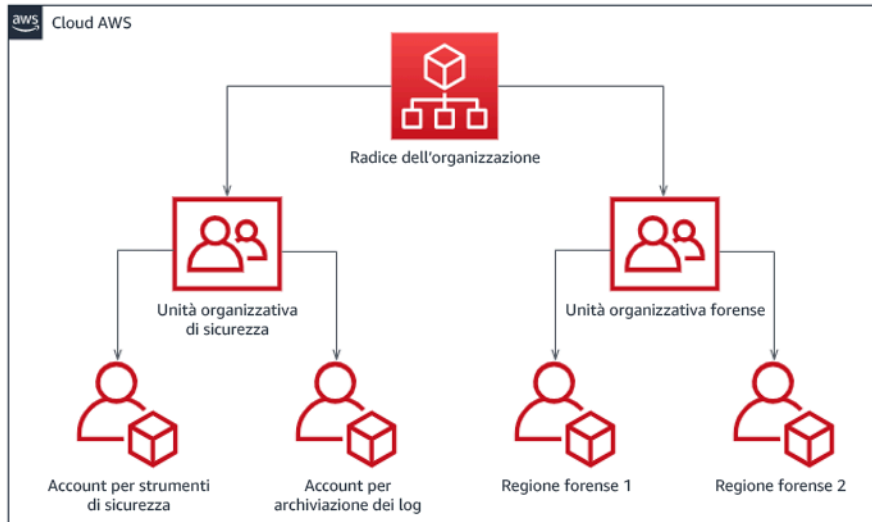
- **Archiviazione dei log:** aggrega i log in un Account AWS di archiviazione dei log con autorizzazioni limitate.
- **Strumenti di sicurezza:** centralizza i servizi di sicurezza in un Account AWS dello strumento di sicurezza. Questo account funge da amministratore delegato per i servizi di sicurezza.

Nell'unità organizzativa di funzionalità forensi, hai la possibilità di implementare uno o più account di funzionalità forensi per ogni regione in cui operi, a seconda di quale è più adatta all'azienda e al modello operativo. Se crei un account di funzionalità forensi per regione, puoi bloccare la creazione di risorse AWS al di fuori della regione e ridurre il rischio che le risorse vengano copiate in una regione indesiderata. Ad esempio, se operi solo in US East (N. Virginia) Region (us-east-1) e US West (Oregon) (us-west-2), allora avresti due account nell'unità organizzativa forense: uno per us-east-1 e uno per us-west-2.

Puoi creare un Account AWS di funzionalità forensi per più regioni. Quando si copiano le risorse AWS nell'account occorre prestare attenzione a rispettare i requisiti di sovranità dei dati. Poiché la creazione di nuovi account richiede tempo, è fondamentale creare e strumentare gli account di

funzionalità forensi con largo anticipo rispetto agli incidenti, in modo che gli addetti siano preparati a utilizzarli efficacemente per la risposta.

Il diagramma seguente mostra una struttura degli account di esempio che include un'unità organizzativa di funzionalità forensi con gli account di funzionalità forensi per regione:



Struttura degli account per regione per la risposta agli incidenti

Acquisizione di backup e snapshot

La configurazione dei backup dei sistemi e dei database importanti è fondamentale per il ripristino da un incidente di sicurezza e per scopi forensi. Con i 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 possono supportarti nelle operazioni di backup e ripristino. Per informazioni dettagliate su questi servizi e approcci per il backup e il ripristino, consultare [Guida prescrittiva per il backup e il ripristino](#) e [Usa i backup per il ripristino in seguito a incidenti di sicurezza](#).

Soprattutto in situazioni come un attacco ransomware, è fondamentale che i backup siano ben protetti. Per indicazioni sulla protezione dei backup, consultare [Le 10 migliori pratiche di sicurezza per proteggere i backup in AWS](#). Oltre a proteggere, è necessario eseguire regolarmente i test dei processi di backup e ripristino per verificare che la tecnologia e le 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 le istanze e gli account sono numerosi. Inoltre, la raccolta manuale può essere soggetta all'errore umano. Per questi motivi, è necessario 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 di seguito. Queste risorse sono esempi di modelli di funzionalità forensi che abbiamo sviluppato e che i clienti hanno implementato. Costituiscono un'utile architettura di riferimento per iniziare, ma prendi in considerazione la possibilità di modificarli o creare nuovi modelli di automazione per le funzionalità forensi in base all'ambiente, ai requisiti, agli strumenti e ai 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:

- [Automatizzazione delle indagini e della risposta agli incidenti](#)

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 dallo sviluppo di playbook. I playbook di risposta agli incidenti forniscono una serie di indicazioni

prescrittive e di passaggi da seguire quando si verifica un evento di sicurezza. Avere una struttura e passaggi chiari semplifica la risposta e riduce 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 il Denial of Service (DoS), il ransomware e la compromissione delle credenziali.
- Avvisi o esiti di sicurezza noti: i playbook devono essere creati per gli esiti e gli avvisi di sicurezza noti, ad esempio gli esiti GuardDuty. Potresti ricevere un risultato di GuardDuty e non sapere cosa fare. Per evitare di mal gestire o ignorare un risultato di GuardDuty, crea un playbook per ogni potenziale risultato di GuardDuty. I dettagli e le indicazioni sulla correzione sono disponibili nella [documentazione di GuardDuty](#). Vale la pena notare che GuardDuty non è abilitato per impostazione predefinita e comporta costi. Per maggiori dettagli su GuardDuty, consulta [Appendice A: Definizioni delle capacità del cloud - Visibilità e avvisi](#).

I playbook devono contenere i passaggi tecnici che un analista deve completare per indagare e rispondere adeguatamente a un potenziale incidente di sicurezza.

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 sulla comunicazione e sull'escalation: chi è coinvolto e quali sono le loro informazioni di contatto? Quali sono le responsabilità di ogni stakeholder?
- Fasi 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 deve essere eseguito per ottenere il risultato desiderato?
 - Individuazione: come verrà rilevato 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?
- Recupero: in che modo il sistema o la risorsa interessati verranno riportati in produzione?
- Risultati attesi: 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 il team di risposta agli incidenti disponga degli opportuni diritti di accesso allocati in AWS per ridurre i tempi necessari per l'analisi e il ripristino.

Anti-pattern comuni:

- L'utilizzo dell'account root per la risposta agli incidenti.
- La modifica degli account utente esistenti.
- La 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 le attività di risposta agli incidenti, consigliamo 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. Se la richiesta viene approvata, l'utente riceve un set di credenziali [AWS temporanee](#) che può utilizzare per eseguire le sue attività. Alla scadenza di queste 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 farlo è utilizzare [AWS Security Token Service](#) e [le policy di sessione](#) per definire l'ambito di accesso.

Esistono scenari in cui le identità federate non sono disponibili, come nei casi di:

- 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 indisponibilità del sistema.

Nei casi precedenti, si deve configurare un accesso di emergenza di tipo break-glass per consentire l'analisi e la tempestiva risoluzione degli incidenti. Ti consigliamo di utilizzare [un utente IAM con le autorizzazioni appropriate](#) per eseguire le attività e accedere alle risorse AWS. Utilizza le credenziali root solo per le [attività che richiedono l'accesso come utente root](#). Per verificare che i team di risposta agli incidenti dispongano del corretto livello di accesso ad AWS e ad altri sistemi pertinenti, ti consigliamo di eseguire la pre-assegnazione di account utente dedicati. Gli account utente richiedono l'accesso con privilegi e devono essere rigorosamente controllati e monitorati. Gli account devono essere 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.

Utilizza 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 rischia di non revocare i 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. Per supportare questa esigenza, crea un playbook per verificare che gli utenti dei team di risposta agli incidenti vengano creati come utenti AWS Identity and Access Management in un account di sicurezza dedicato e non gestiti tramite

una federazione esistente o una soluzione di autenticazione unica (SSO). Ogni singolo utente dei team di risposta deve avere il proprio account denominato. La configurazione dell'account deve applicare [una policy di password complesse](#) e l'autenticazione a più fattori (MFA). Se i playbook di risposta agli incidenti richiedono solo l'accesso alla AWS Management Console, non è necessario che l'utente disponga di chiavi di accesso configurate né che sia esplicitamente autorizzato a creare chiavi di accesso. A tale scopo è possibile configurare le policy IAM o le policy di controllo dei servizi come menzionato in AWS Security Best Practices (Best practice di sicurezza AWS) per [le policy di controllo dei servizi AWS Organizations](#). Gli utenti non devono avere privilegi oltre la 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 che qualsiasi accesso aggiuntivo venga revocato immediatamente dopo il completamento dell'incidente.

Per verificare che l'uso dei ruoli di risposta agli incidenti possa essere adeguatamente monitorato e controllato, è essenziale che gli account utente IAM creati a tale scopo non siano condivisi tra le persone e che l'utente root Account AWS non venga utilizzato se [non 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 della password dell'utente root e del token MFA.

Per configurare le policy IAM per i ruoli di risposta agli incidenti, prendi in considerazione di usare [IAM Access Analyzer](#) per generare le policy sulla base dei log AWS CloudTrail. In questo caso, concedi l'accesso come amministratore al ruolo di risposta agli incidenti per un account non di produzione ed esegui i playbook. Al termine, potrà essere creata una policy che consenta solo le azioni da intraprendere. Questa policy può quindi essere applicata a tutti i ruoli di risposta agli incidenti in tutti gli account. Puoi anche creare una policy IAM separata per ogni playbook per avere una gestione e un controllo più semplici. Esempi di playbook possono essere piani di risposta per ransomware, violazioni dei dati, perdita dell'accesso alla produzione e altri scenari.

Utilizza gli account utente di risposta agli incidenti per assumere i ruoli di risposta [IAM dedicati 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 nominare chiaramente gli account utente IAM e i ruoli IAM per trovarli facilmente nei log CloudTrail. Un esempio potrebbe essere quello di nominare gli account IAM `<ID_UTENTE>-BREAK-GLASS` e i ruoli IAM `RUOLO-BREAK-GLASS`.

[CloudTrail](#) viene utilizzato per registrare l'attività API negli account AWS e deve essere 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. Le istruzioni possono essere modificate per configurare il parametro [Amazon CloudWatch](#) da filtro a filtro negli eventi `AssumeRole` correlati al ruolo IAM di risposta agli incidenti:

```
{ $.eventName = "AssumeRole" && $.requestParameters.roleArn =  
  "<ARN_RUOLO_DI_RISPOSTA_AGLI_INCIDENTI>" && $.userIdentity.invokedBy NOT EXISTS &&  
  $.eventType != "AwsServiceEvent" }
```

Poiché è probabile 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 vengano gestiti tempestivamente.

Durante un incidente, è possibile che un membro del team di risposta richieda l'accesso a sistemi che non sono direttamente protetti da IAM, ad esempio istanze Amazon Elastic Compute Cloud, database Amazon Relational Database Service o piattaforme Software-as-a-service (SaaS). Anziché i protocolli nativi come SSH o RDP, ti consigliamo vivamente di utilizzare [AWS Systems Manager Session Manager](#) per l'accesso amministrativo completo alle istanze Amazon EC2. Questo accesso può essere monitorato utilizzando IAM, che è sicuro e controllato. Puoi anche automatizzare parti dei tuoi playbook utilizzando i documenti di [AWS Systems Manager Run Command](#) che possono ridurre gli errori dell'utente 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 AWS Secrets Manager e di concedere l'accesso ai ruoli degli utenti dei team di risposta agli incidenti.

Infine, la gestione degli account utente IAM di risposta agli incidenti deve essere aggiunta ai processi [degli utenti che si uniscono, si spostano o lasciano l'organizzazione](#) e deve rivista e testata periodicamente per verificare che sia consentito solo l'accesso previsto.

Risorse

Documenti correlati:

- [Managing temporary elevated access to your AWS environment \(Gestione dell'accesso temporaneo con privilegi elevati all'ambiente AWS\)](#)
- [AWS Security Incident Response Guide \(Guida alle risposte agli incidenti di sicurezza di AWS\)](#)

- [AWS Elastic Disaster Recovery](#)
- [AWS Systems Manager Incident Manager](#)
- [Impostazione di una policy delle password dell'account per utenti IAM](#)
- [Utilizzo dell'autenticazione a più fattori \(MFA\) in AWS](#)
- [Configuring Cross-Account Access with MFA \(Configurazione dell'accesso multi-account con MFA\)](#)
- [Using IAM Access Analyzer to generate IAM policies \(Utilizzo di IAM Access Analyzer per generare policy IAM\)](#)
- [Best Practices for AWS Organizations Service Control Policies in a Multi-Account Environment \(Best practice per le policy di controllo dei servizi di AWS Organizations in un ambiente multi-account\)](#)
- [How to Receive Notifications When Your AWS Account's Root Access Keys Are Used \(Come ricevere le notifiche quando vengono utilizzate le chiavi di accesso root dell'account AWS\)](#)
- [Create fine-grained session permissions using IAM managed policies \(Creazione di autorizzazioni di sessione dettagliate utilizzando le policy gestite da IAM\)](#)

Video correlati:

- [Automating Incident Response and ForensicsAWS](#)
- [DIY guide to runbooks, incident reports, and incident response](#)
- [Prepare for and respond to security incidents in your AWS environment](#)

Esempi correlati:

- [Lab: AWS Account Setup and Root User \(Laboratorio: configurazione dell'account AWS e dell'utente root\)](#)
- [Lab: Incident Response with AWS Console and CLI \(Laboratorio: risposta agli incidenti con la Console AWS e l'interfaccia della riga di comando\)](#)

SEC10-BP06 Distribuzione anticipata degli strumenti

Verifica che il team addetto alla sicurezza disponga degli strumenti giusti pre-distribuiti 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, invece di far monitorare alle persone il comportamento di sicurezza e reagire manualmente agli eventi.

Se i team di risposta agli incidenti continuano a rispondere agli avvisi nello stesso modo, rischiano il cosiddetto affaticamento dagli avvisi ("alert fatigue"). Ciò significa che, nel corso del tempo, il team può diventare desensibilizzato agli avvisi e può commettere errori nella gestione di situazioni ordinarie o farsi sfuggire avvisi insoliti. L'automazione aiuta a evitare l'affaticamento dagli avvisi utilizzando funzioni che elaborano gli avvisi ripetitivi e ordinari, lasciando alle persone la gestione degli incidenti sensibili e univoci. Se si integrano sistemi di rilevamento delle anomalie, come Amazon GuardDuty, AWS CloudTrail Insights e Amazon CloudWatch Anomaly Detection, è possibile 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 decomporre tale modello in una logica fruibile e scrivere il codice per eseguire tale logica. 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 sono necessari anche per la generazione di avvisi, che indicano che sono avvenute determinate azioni di interesse. È fondamentale selezionare, attivare, memorizzare e impostare i meccanismi di query e recupero e impostare gli avvisi. Inoltre, un modo efficace per fornire gli strumenti per la ricerca nei dati di log è [Amazon Detective](#).

AWS offre oltre 200 servizi cloud e migliaia di funzionalità. Ti consigliamo di esaminare i servizi che possono supportare e semplificare la tua strategia di risposta agli incidenti.

Oltre ai log, è necessario sviluppare e implementare una [strategia di applicazione dei tag](#). L'applicazione dei tag può aiutare a fornire il contesto per lo scopo di una risorsa AWS. I tag può essere utilizzati anche per l'automazione.

Passaggi dell'implementazione

Seleziona e configura i log per l'analisi e gli avvisi

Consulta la seguente documentazione sulla configurazione dei log per la risposta agli incidenti:

- [Logging strategies for security incident response](#)
- [SEC04-BP01 Configurazione dei registri di servizi e applicazioni](#)

Abilitazione dei servizi di sicurezza per supportare il rilevamento e la risposta

AWS offre funzionalità investigative, preventive e reattive native e altri servizi che possono essere utilizzati 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](#).

Sviluppa e implementa una strategia di tag

Ottenere informazioni contestuali sul caso d'uso aziendale e sugli stakeholder interni pertinenti relativi a una risorsa AWS può essere difficile. Un modo per farlo è rappresentato dai 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 tag coerente può accelerare la 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 etichettare, consulta [Etichettare le tue risorse AWS](#). Dovrai prima definire i tag nella tua organizzazione e quindi implementare e applicare questa strategia di tag. Per maggiori dettagli sull'implementazione e l'applicazione, consulta [Implementa una strategia di etichettatura delle risorse AWS utilizzando AWS Tag Policies and Service Control Policies \(SCPs\)](#).

Risorse

Best practice Well-Architected correlate:

- [SEC04-BP01 Configurazione dei registri di servizi e applicazioni](#)
- [SEC04-BP02 Analisi di log, risultati e parametri a livello centrale](#)

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](#)
- [Security Hub Workshop](#)
- [Vulnerability Management with 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 alla mancata adozione di questa best practice: 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.

- **Esercizi del 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 (pen-test) 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 lo scenario 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.
- **Esercizi del 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 del team rosso possono basarsi su test invasivi, sii cauto 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'esercizio: definisci lo scenario di simulazione e gli obiettivi della simulazione. Lo scenario e gli obiettivi dovrebbero essere entrambi accettati dalla leadership.

2. Identifica le principali parti interessate: come minimo, un esercizio richiede la presenza di facilitatori 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. Facilita 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. Sviluppa il report post-azione (AAR): individua le aree che sono andate bene, quelle che possono essere migliorate 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:

- [AWS Incident Response Guide](#)

Video correlati:

- [AWS GameDay - Security Edition](#)

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 sono disponibili nella tabella seguente.

Fase	Obiettivo
Rilevamento	Identifica un potenziale evento di sicurezza.

Fase	Obiettivo
Analisi	Determina se l'evento di sicurezza è un incidente e valutarne 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.
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. Quindi, segui le best practice della sezione [Preparazione](#) per poter rispondere efficacemente a un evento di sicurezza attivo.

Per maggiori informazioni, consulta la sezione [Operazioni](#) della Guida sulla risposta agli incidenti di sicurezza di AWS

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 che stabilisce e raggiunge, ad alto livello, 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 dimensionare 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?
 - Il personale presentava lacune nella formazione o nelle capacità necessarie per rispondere e indagare efficacemente sull'incidente?
 - Le risorse appropriate erano pronte e disponibili?
 - Elaborazione
 - 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 gli stakeholder.

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.

I costi e la complessità associati alla correzione dei difetti sono in genere inferiori se ti trovi 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.

Queste linee guida di implementazione sono incentrate su quattro aree: organizzazione e cultura, sicurezza della pipeline, sicurezza nella pipeline e gestione delle dipendenze. Ogni 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 \(pen-test\) a intervalli regolari](#)
- [SEC11-BP04 Revisioni manuali 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

Fornisci formazione sulle procedure comuni agli sviluppatori nell'organizzazione in modo da garantire la sicurezza dello sviluppo e del funzionamento delle applicazioni. L'adozione di procedure di sviluppo incentrate sulla sicurezza riduce la probabilità di riscontrare problemi solo nella fase di revisione della sicurezza.

Risultato desiderato: progettazione del software tenendo conto della sicurezza. Quando gli sviluppatori in un'organizzazione ricevono formazione su procedure di sviluppo sicure iniziando con un modello di rischio, la qualità e la sicurezza complessive del software prodotto sono migliori. Questo approccio può ridurre il tempo necessario per distribuire il software o le funzionalità, in quanto saranno necessarie meno correzioni dopo la fase di revisione della sicurezza.

Ai fini di questa best practice, il concetto di sviluppo sicuro si riferisce al software scritto e agli strumenti o ai sistemi che supportano il ciclo di vita di sviluppo del software.

Anti-pattern comuni:

- Valutazione delle proprietà di sicurezza di un sistema solo in fase di revisione della sicurezza.
- Assegnazione di tutte le decisioni in materia di sicurezza al team responsabile della sicurezza.
- Mancata comunicazione della correlazione tra le decisioni adottate durante il ciclo di vita di sviluppo del software e le aspettative o policy complessive dell'organizzazione.
- Svolgimento del 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 alla mancata adozione di questa best practice: medio

Guida all'implementazione

Fornisci formazione agli sviluppatori nell'organizzazione. Un corso iniziale sulla [modellazione delle minacce](#) è un'ottima base per la formazione sulla sicurezza. Idealmente, gli sviluppatori devono poter accedere in modalità self-service a informazioni pertinenti ai propri carichi di lavoro. Questo accesso può aiutarli a prendere decisioni informate sulle proprietà di sicurezza dei sistemi sviluppati senza dover chiedere a un altro team. Il processo di coinvolgimento del team responsabile della sicurezza nelle revisioni deve essere definito chiaramente e facile da seguire. Le fasi del processo di revisione devono essere incluse nella formazione sulla sicurezza. Quando sono disponibili modelli o schemi di implementazione noti, devono essere facili da trovare e collegare ai requisiti complessivi per la sicurezza. Valuta se usare [AWS CloudFormation](#), [costrutti del AWS Cloud Development Kit \(AWS CDK\)](#), il [Service Catalog](#) o altri strumenti di creazione di modelli per ridurre la necessità di configurazioni personalizzate.

Passaggi dell'implementazione

- Per iniziare, presenta agli sviluppatori un corso sulla [modellazione delle minacce](#) per creare ottime basi e abituarli a riflettere sulla sicurezza.
- Fornisci accesso a risorse di formazione [AWS Training and Certification](#), per i diversi settori o per partner AWS.
- Fornisci formazione sul processo di revisione della sicurezza dell'organizzazione, che spieghi la suddivisione delle responsabilità tra il team responsabile della sicurezza, i team del carico di lavoro e altri stakeholder.
- Pubblica linee guida self-service su come soddisfare i requisiti di sicurezza, inclusi esempi e modelli di codice, se disponibili.
- Richiedi regolarmente ai team di sviluppo feedback sull'esperienza durante il processo di revisione della sicurezza e la formazione correlata e usalo per migliorare le procedure.

- Usa campagne di simulazione o bug bash per ridurre il numero di problemi e migliorare le competenze degli sviluppatori.

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](#)
- [Come riflettere sulla governance della sicurezza nel cloud](#)
- [Come accostarsi alla modellazione delle minacce](#)
- [Accelerazione della formazione – AWS Skills Guild](#)

Video correlati:

- [Sicurezza proattiva: considerazioni e approcci](#)

Esempi correlati:

- [Workshop sulla modellazione delle minacce](#)
- [Industry awareness for developers](#)

Servizi correlati:

- [AWS CloudFormation](#)
- [Costrutti del AWS Cloud Development Kit \(AWS CDK\) \(AWS CDK\)](#)
- [Service Catalog](#)
- [AWS BugBust](#)

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 automatici è fornire un metodo programmatico per rilevare inizialmente e regolarmente i potenziali problemi lungo l'intero ciclo di vita di 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 unit test 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 test case 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 di 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 unit test sono le più adatte per l'automazione. L'automazione dei test delle proprietà di sicurezza permette agli sviluppatori di ricevere automaticamente 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 test case e dei risultati dei test automatici.
- Esecuzione dei test solo immediatamente prima di un rilascio.
- Automazione dei test case 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 risultati uniformi tra più flussi di lavoro.
- Minore probabilità di introdurre problemi di sicurezza nel software di produzione.

- Intervallo di tempo più breve tra il rilevamento e la correzione grazie all'identificazione più tempestiva dei problemi software.
- Maggiore visibilità su comportamenti sistematici o ripetuti tra più flussi di lavoro, che può essere usata per favorire miglioramenti in tutta l'organizzazione.

Livello di rischio associato alla mancata adozione di questa best practice: 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 per un codice privo di 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](#) offre un confronto tra gli [analizzatori della sicurezza del codice sorgente](#), con 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 imprevedibili. I test dinamici possono essere usati per 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 CodeWhisperer](#) fornisce suggerimenti per il codice, tra cui analisi della sicurezza, nell'ambiente di sviluppo integrato (IDE) dello sviluppatore. Il [Amazon CodeGuru Reviewer](#) può identificare problemi critici e di sicurezza e bug difficili da individuare durante lo sviluppo delle applicazioni e fornisce suggerimenti per migliorare la qualità del codice.

Il [workshop sulla sicurezza per gli sviluppatori](#) usa strumenti di sviluppo AWS come [AWS CodeBuild](#), [AWS CodeCommit](#) e [AWS CodePipeline](#) per l'automazione della pipeline di rilascio, che include metodologie di test tramite analisi statiche e dinamiche.

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 appropriato bloccare le pipeline anziché informare semplicemente gli sviluppatori riguardo alla necessità di risolvere i problemi.
- Il [workshop sulla sicurezza per gli sviluppatori](#) fornisce un esempio di integrazione di test statici e dinamici in una pipeline di rilascio.
- L'esecuzione di test o di analisi del codice tramite strumenti automatici, come [Amazon CodeWhisperer](#) integrato con gli ambienti IDE degli sviluppatori e il [Amazon CodeGuru Reviewer](#) per l'analisi del codice in fase di commit, permette agli sviluppatori di ottenere feedback tempestivo.
- Se sviluppi soluzioni usando AWS Lambda, puoi usare [Amazon Inspector](#) per analizzare il codice dell'applicazione nelle funzioni.
- Il [workshop sull'integrazione continua e sulla distribuzione continua in AWS](#) fornisce un punto di partenza per la creazione di pipeline CI/CD in AWS.
- Quando 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 risultati, il collegamento a linee guida per la correzione permette agli sviluppatori di migliorare la qualità del codice.
- Analizza regolarmente i risultati ottenuti dagli strumenti automatici per definire le priorità delle successive iniziative di automazione, formazione degli sviluppatori o creazione di campagne di sensibilizzazione.

Risorse

Documenti correlati:

- [Distribuzione e implementazione continue](#)
- [Partner con competenze in AWS DevOps](#)

- [Partner con competenze nella sicurezza AWS](#) per la sicurezza delle applicazioni
- [Scelta di un approccio CI/CD Well-Architected](#)
- [Monitoraggio di eventi CodeCommit in Amazon EventBridge e Amazon CloudWatch Events](#)
- [Rilevamento dei segreti nel revisore Amazon CodeGuru](#)
- [Accelerazione delle implementazioni su AWS con una governance efficace](#)
- [Approccio di AWS all'automazione di implementazioni pratiche e sicure](#)

Video correlati:

- [Informazioni pratiche: automazione di pipeline di distribuzione continua in Amazon](#)
- [Automazione di pipeline CI/CD tra account](#)

Esempi correlati:

- [Industry awareness for developers](#)
- [AWS CodePipeline Governance](#) (GitHub)
- [Workshop sulla sicurezza per gli sviluppatori](#)
- [Workshop sull'integrazione continua e sulla distribuzione continua in AWS](#)

SEC11-BP03 Esecuzione di test di penetrazione (pen-test) a intervalli regolari

Esegui regolarmente test di penetrazione (pen-test) sul software. Questo meccanismo permette di identificare i potenziali problemi che non possono essere rilevati tramite test automatici o la revisione manuale del codice. Può anche aiutarti a determinare l'efficacia dei controlli di rilevamento. I test di penetrazione (pen-test) devono determinare se il software può funzionare in modi imprevisti, ad esempio esponendo dati che devono essere protetti o concedendo autorizzazioni più elevate del previsto.

Risultato desiderato: uso di test di penetrazione (pen-test) per rilevare, correggere e convalidare le proprietà di sicurezza dell'applicazione. È necessario eseguire test di penetrazione (pen-test) regolari e pianificati come parte del ciclo di vita di sviluppo del software. I risultati ottenuti dai test di penetrazione (pen-test) devono essere affrontati prima del rilascio del software. Devi analizzare i risultati dei test di penetrazione (pen-test) per identificare se vi siano problemi che possono essere

identificati con l'automazione. Un processo di esecuzione di test di penetrazione (pen-test) regolare e ripetibile che includa 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 (pen-test) solo per problemi di sicurezza noti o comuni.
- Esecuzione di test di penetrazione (pen-test) delle applicazioni senza gli strumenti e le librerie di terze parti dipendenti.
- Esecuzione di test di penetrazione (pen-test) 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 alla mancata adozione di questa best practice: elevato

Guida all'implementazione

I test di penetrazione (pen-test) 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 (pen-test) iniziano dalla ricognizione, durante la quale vengono raccolti 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 accesso accidentale all'ambiente o accesso non autorizzato ai dati. Devi eseguire test di penetrazione (pen-test) quando avvii 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 (pen-test). 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

- Prepara un processo strutturato per definire l'ambito dei test di penetrazione (pen-test). Un ottimo metodo per mantenere il contesto consiste nel basare questo processo sul [modello di rischio](#).
- Identifica la fase più appropriata del ciclo di vita di sviluppo in cui eseguire test di penetrazione (pen-test). 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 dai risultati dei test di penetrazione (pen-test) e su come ottenere informazioni sulla correzione.
- Usa strumenti per accelerare il processo di esecuzione dei test di penetrazione (pen-test) automatizzando test comuni o ripetibili.
- Analizza i risultati dei test di penetrazione (pen-test) 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 [Test di penetrazione \(pen-test\) AWS](#) fornisce linee guida dettagliate per l'esecuzione di test di penetrazione (pen-test) in AWS
- [Accelerazione delle implementazioni su AWS con una governance efficace](#)
- [Partner con competenze nella sicurezza AWS](#)
- [Modernizzazione dell'architettura dei test di penetrazione \(pen-test\) su AWS Fargate](#)
- [Simulatore di iniezione guasti AWS](#)

Esempi correlati:

- [Automate API testing with AWS CodePipeline](#) (GitHub)
- [Automated security helper](#) (GitHub)

SEC11-BP04 Revisioni manuali del codice

Esegui una revisione manuale del codice del software che produci. Attraverso questo processo puoi assicurarti che chi ha scritto il codice non sia l'unica persona a controllarne la qualità.

Risultato desiderato: l'aggiunta di una fase di revisione manuale del codice durante lo sviluppo migliora la qualità del software scritto, permette di affinare le competenze dei membri meno esperti del team e fornisce un'opportunità per identificare i punti in cui può essere usata l'automazione. Le revisioni manuali del codice possono essere supportate da strumenti e test automatici.

Anti-pattern comuni:

- Non viene eseguita alcuna revisione del codice prima dell'implementazione.
- La scrittura e la revisione del codice vengono effettuate dalla stessa persona.
- Non viene usata l'automazione per semplificare o orchestrare le revisioni del codice.
- Gli sviluppatori non ricevono formazione 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 alla mancata adozione di questa best practice: medio

Guida all'implementazione

La fase di revisione deve essere implementata come parte del flusso complessivo di gestione del codice. Le specifiche dipendono dall'approccio usato per la diramazione, le richieste pull e l'unione. Puoi usare AWS CodeCommit o soluzioni di terze parti come GitHub, GitLab o Bitbucket. Qualunque

sia il metodo usato, è importante verificare che i processi richiedano la revisione del codice prima che venga implementato in un ambiente di produzione. L'uso di strumenti come il [Amazon CodeGuru Reviewer](#) può semplificare l'orchestrazione del processo di revisione del codice.

Passaggi dell'implementazione

- Implementa una fase di revisione manuale come parte del flusso di gestione del codice ed esegui la revisione prima di continuare.
- Prendi in considerazione il [Amazon CodeGuru Reviewer](#) per la gestione e la semplificazione delle revisioni del codice.
- Implementa un flusso di approvazione che richieda il completamento di una revisione prima che il codice possa passare alla fase successiva.
- Verifica che sia stato definito un processo per identificare i problemi riscontrati durante le revisioni manuali del codice che potrebbero essere rilevati automaticamente.
- Integra la fase di revisione manuale del codice in modo che sia allineata alla procedure di sviluppo del codice.

Risorse

Best practice correlate:

- [SEC11-BP02 Automazione dei test lungo il ciclo di vita di sviluppo e test](#)

Documenti correlati:

- [Uso di richieste pull in repository AWS CodeCommit](#)
- [Uso di modelli per le regole di approvazione in AWS CodeCommit](#)
- [GitHub: About pull requests](#)
- [Automazione delle revisioni del codice con il Amazon CodeGuru Reviewer](#)
- [Automazione del rilevamento di bug e vulnerabilità della sicurezza in pipeline CI/CD usando l'interfaccia della riga di comando del Amazon CodeGuru Reviewer](#)

Video correlati:

- [Miglioramento continuo della qualità del codice con Amazon CodeGuru](#)

Esempi correlati:

- [Workshop sulla sicurezza per gli sviluppatori](#)

SEC11-BP05 Centralizzazione dei servizi per pacchetti e dipendenze

Fornisci servizi centralizzati per permettere ai team di sviluppo 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 software include una serie di altri pacchetti software oltre al codice scritto. In questo modo, è più facile utilizzare implementazioni di funzionalità usate ripetutamente, come un parser JSON o una libreria di crittografia. La centralizzazione logica delle origini per questi pacchetti e dipendenze fornisce un meccanismo tramite il quale i team responsabili della sicurezza possono convalidare le proprietà dei pacchetti prima che vengano usati. Questo approccio riduce anche il rischio di un problema imprevisto causato da una modifica in un pacchetto esistente o dall'aggiunta da parte dei team di sviluppo di pacchetti arbitrari direttamente da Internet. Usa questo approccio 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 alla mancata adozione di questa best practice: 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. Ti consigliamo di implementare un metodo efficiente per aggiungere pacchetti al repository quando sono necessari aggiornamenti o emergono nuovi requisiti. Servizi AWS come [AWS CodeArtifact](#) o soluzioni simili di partner AWS forniscono alcuni strumenti utili per questo scopo.

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 che vengano pubblicati 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:

- [Accelerazione delle implementazioni su AWS con una governance efficace](#)
- [Potenziamento della sicurezza dei pacchetti con il toolkit per il controllo delle origini dei pacchetti CodeArtifact](#)
- [Rilevamento dei problemi di sicurezza nella registrazione con il Amazon CodeGuru Reviewer](#)

- [Supply chain Levels for Software Artifacts \(SLSA\)](#)

Video correlati:

- [Sicurezza proattiva: considerazioni e approcci](#)
- [La filosofia di AWS per la sicurezza \(re:Invent 2017\)](#)
- [Quando sicurezza, protezione e urgenza sono tutte importanti: gestione di Log4Shell](#)

Esempi correlati:

- [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)

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: un intervento minimo sui dati da parte delle persone è un principio chiave dello sviluppo sicuro nel Cloud AWS. Questo principio include anche il modo in cui viene implementato il software.

I vantaggi legati alla scelta di non affidare a persone l'implementazione del software è la migliore garanzia che la soluzione implementata sia esattamente identica a quella testata e che l'implementazione verrà eseguita in modo coerente ogni volta. Il software non deve essere modificato in modo da funzionare in ambienti diversi. Usando i principi dello sviluppo di applicazioni a dodici fattori, in particolare l'esternalizzazione della configurazione, puoi implementare lo stesso codice in più ambienti senza richiedere modifiche. La firma crittografica dei pacchetti software è un ottimo metodo per verificare che non vengano apportate modifiche tra ambienti. Il risultato complessivo di questo approccio è la riduzione dei rischi nel processo di modifica e il miglioramento della coerenza delle versioni del software.

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 ripristino automatico dello stato precedente 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 alla mancata adozione di questa best practice: elevato

Guida all'implementazione

Crea la struttura di Account AWS per eliminare l'accesso umano frequente dagli ambienti e usa strumenti CI/CD per eseguire le implementazioni. Progetta le applicazioni in modo da ottenere i dati di configurazione specifici dell'ambiente da un'origine esterna, ad esempio l'[Archivio dei parametri AWS Systems Manager](#). Firma i pacchetti dopo che vengono testati e convalida le firme durante l'implementazione. Configura le pipeline CI/CD per il push del codice delle applicazioni e usa valori Canary per confermare la corretta esecuzione dell'implementazione. Usa strumenti come [AWS CloudFormation](#) o il [AWS CDK](#) per definire l'infrastruttura, quindi [AWS CodeBuild](#) e [AWS CodePipeline](#) per eseguire operazioni CI/CD.

Passaggi dell'implementazione

- Crea pipeline CI/CD ben definite per semplificare il processo di implementazione.
- L'uso di [AWS CodeBuild](#) e [AWS Code Pipeline](#) per fornire funzionalità CI/CD semplifica l'integrazione di test di sicurezza nelle pipeline.
- Segui le linee guida sulla separazione degli ambienti nel whitepaper sull'[organizzazione dell'ambiente AWS usando più account](#).
- Verifica che non si verifichi accesso umano frequente agli ambienti in cui sono in esecuzione carichi di lavoro di produzione.
- Progetta le applicazioni in modo che supportino l'esternalizzazione dei dati di configurazione.

- Valuta se eseguire l'implementazione usando un modello di implementazione blu/verde.
- Implementa valori Canary per convalidare la corretta implementazione del software.
- Usa strumenti di crittografia come [AWS Signer](#) o [AWS Key Management Service \(AWS KMS\)](#) per firmare e verificare i pacchetti software implementati.

Risorse

Best practice correlate:

- [SEC11-BP02 Automazione dei test lungo il ciclo di vita di sviluppo e test](#)

Documenti correlati:

- [Workshop sull'integrazione continua e sulla distribuzione continua in AWS](#)
- [Accelerazione delle implementazioni su AWS con una governance efficace](#)
- [Automazione di implementazioni pratiche e sicure](#)
- [Firma del codice usando l'Autorità privata per la gestione del certificato AWS \(ACM CA privata/ ACM PCA\) e chiavi asimmetriche AWS Key Management Service](#)
- [Firma del codice, un controllo di attendibilità e integrità per AWS Lambda](#)

Video correlati:

- [Informazioni pratiche: automazione di pipeline di distribuzione continua in Amazon](#)

Esempi correlati:

- [Implementazioni blu/verde con AWS Fargate](#)

SEC11-BP07 Valutazione regolare delle proprietà di sicurezza delle pipeline

Applica i principi della sicurezza Well-Architected alle pipeline, con particolare attenzione alla separazione delle autorizzazioni. Valuta regolarmente le proprietà di sicurezza dell'infrastruttura di pipeline. Una gestione efficace della sicurezza delle pipeline assicura la protezione del software che passa attraverso le pipeline.

Risultato desiderato: le pipeline usate per sviluppare e implementare il software devono seguire le stesse procedure consigliate di qualsiasi altro carico di lavoro nell'ambiente. I test implementati nelle pipeline non devono essere modificabili dagli sviluppatori che li usano. Le pipeline devono avere solo le autorizzazioni necessarie per le implementazioni eseguite e devono applicare misure di protezione per evitare l'implementazione negli ambienti errati. Le pipeline non devono basarsi su credenziali a lungo termine e devono essere configurate in modo da emettere lo stato, per permettere la convalida dell'integrità degli ambienti di sviluppo.

Anti-pattern comuni:

- Test di sicurezza che possono essere ignorati 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 alla mancata adozione di questa best practice: elevato

Guida all'implementazione

Iniziando con servizi CI/CD gestiti che supportano ruoli IAM, puoi ridurre il rischio di perdita di credenziali. L'applicazione dei principi della sicurezza all'infrastruttura di pipeline CI/CD può aiutarti a determinare i punti in cui apportare miglioramenti per la sicurezza. Un ottimo punto di partenza per la creazione degli ambienti CI/CD è l'[architettura di riferimento per le pipeline di implementazione AWS](#). La revisione periodica dell'implementazione delle pipeline e l'analisi dei log per identificare comportamenti imprevisti può semplificare la comprensione dei modelli di utilizzo delle pipeline usate per implementare il software.

Passaggi dell'implementazione

- Inizia dall'[architettura di riferimento per le pipeline di implementazione AWS](#).

- Valuta se usare il [AWS IAM Access Analyzer](#) per generare in modo programmatico policy IAM con privilegi minimi per le pipeline.
- Integra le pipeline con monitoraggio e generazione di avvisi in modo da ricevere notifiche in caso di attività imprevista o anomala, in quanto [Amazon EventBridge](#) per servizi gestiti AWS permette di instradare dati a destinazioni come [AWS Lambda](#) o [Amazon Simple Notification Service](#) (Amazon SNS).

Risorse

Documenti correlati:

- [Architettura di riferimento per pipeline di implementazione AWS](#)
- [Monitoraggio di AWS CodePipeline](#)
- [Best practice per la 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 responsabile della sicurezza dovrà convalidare queste decisioni durante una revisione, ma l'integrazione della titolarità della sicurezza nei team di sviluppo permette 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: per integrare la titolarità della sicurezza e il processo decisionale nei team di sviluppo, puoi insegnare agli sviluppatori come riflettere sulla sicurezza o puoi migliorarne la formazione attraverso l'integrazione o l'associazione di responsabili della sicurezza nei team di sviluppo. Entrambi gli approcci sono validi e permettono al team di prendere decisioni di qualità migliore sulla sicurezza nelle fasi iniziali del ciclo di sviluppo. Questo modello di titolarità è basato sulla formazione per la sicurezza delle applicazioni. Iniziando dal modello di rischio per il carico di lavoro specifico, puoi concentrarti sul design thinking nel contesto appropriato. Un altro vantaggio

della presenza di una comunità di sviluppatori attenti alla sicurezza o di un gruppo di tecnici della sicurezza che collabora con i team di sviluppo è la possibilità di comprendere a pieno il modo in cui è compilato il codice. Questa comprensione permette di determinare le aree di miglioramento successive per l'automazione.

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 scritto.
- Opportunità di identificare e comprendere i problemi sistematici o le aree di miglioramento a valore elevato.
- Riduzione della quantità di attività di correzione dovute ai risultati delle revisioni della sicurezza.
- Migliore percezione della funzione della sicurezza.

Livello di rischio associato alla mancata adozione di questa best practice: basso

Guida all'implementazione

Per iniziare, segui le linee guida fornite 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 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, fornisci formazione sulla sicurezza delle applicazioni agli sviluppatori.
- Crea una comunità e un programma di onboarding per preparare 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 rilevanti.
- Tieni traccia delle metriche per il numero di persone coinvolte nel programma, il tempo impiegato per le revisioni e il 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:

- [Come accostarsi alla modellazione delle minacce](#)
- [Come riflettere sulla governance della sicurezza nel cloud](#)

Video correlati:

- [Sicurezza proattiva: considerazioni e approcci](#)

Conclusione

La sicurezza è una sfida costante. Quando si verificano 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. Ciò risulta più semplice grazie alle funzionalità programmatiche e alle caratteristiche e ai servizi AWS discussi in questo documento.

AWS si impegna ad aiutarti a creare e gestire architetture che proteggano informazioni, sistemi e asset offrendo valore aziendale aggiunto.

Collaboratori

Hanno contribuito alla stesura di questo documento:

- Sarita Dharankar, Security Pillar Lead, Well-Architected, Amazon Web Services
- Adam Cerini, Senior Solution Architect, Amazon Web Services
- Bill Shinn, Senior Principal, Office of the CISO, Amazon Web Services
- Brigid Johnson, Senior Software Development Manager, AWS Identity, Amazon Web Services
- Byron Pogson, Senior Solution Architect, Amazon Web Services
- Charlie Hammell, Principal Enterprise Architect, Amazon Web Services
- Darran Boyd, Principal Security Solutions Architect, Financial Services, Amazon Web Services
- Dave Walker, Principal Specialist Solutions Architect, Security and Compliance, Amazon Web Services
- John Formento, Senior Solution Architect, Amazon Web Services
- Paul Hawkins, Principal, Office of the CISO, Amazon Web Services
- Sam Elmalak, Senior Technology Leader, Amazon Web Services
- Pat Gaw, Principal Security Consultant, Amazon Web Services
- Daniel Begimher, Senior Consultant, Security, Amazon Web Services
- Danny Cortegaca, Senior Security Solutions Architect, Amazon Web Services
- Ana Malhotra, Security Solutions Architect, Amazon Web Services
- Debashis Das, Principal, Office of the CISO, Amazon Web Services
- Reef Dsouza, Principal Solutions Architect, Amazon Web Services
- Brad Burnett, Security Solutions Architect, Identity, Amazon Web Services
- Anna McAbee, Senior Security Solutions Architect, Threat Detection and Incident Response, Amazon Web Services
- Jason Garman, Principal Security Solutions Architect, Amazon Web Services

Approfondimenti

Per ulteriore assistenza, consulta le seguenti risorse:

- [Whitepaper – Framework AWS Well-Architected](#)
- [Centro di progettazione AWS](#)

Revisioni del documento

Per ricevere una notifica sugli aggiornamenti di questo 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: Gestione sicura dei carichi di lavoro e Protezione dei dati in transito .	December 6, 2023
Linee guida sulle best practice aggiornate	Principali aggiornamenti alle linee guida e alle best practice per la risposta agli incidenti . Diverse best practice aggiornate nella attività di preparazione . Sono state aggiunte due nuove aree alla risposta agli incidenti: Operazioni e Attività post-incidente . È stata aggiunta la nuova best practice SEC10-BP08 Definizione di un framework per apprendere dagli incidenti .	October 3, 2023
Linee guida sulle best practice aggiornate	Le best practice sono state aggiornate con nuove linee guida nelle aree relative a preparazione e simulazione .	July 13, 2023
Aggiornamenti per il nuovo framework.	Best practice aggiornate con prontuario e nuove best practice aggiunte. È stata	April 10, 2023

	aggiunta una nuova area di best practice per Application Security (AppSec).	
Whitepaper aggiornato	Best practice aggiornate con nuova guida all'implementazione.	December 15, 2022
Whitepaper aggiornato	Ampliamento delle best practice e aggiunta dei piani di miglioramento.	October 20, 2022
Aggiornamento di minore entità	Informazioni IAM aggiornate e per allineamento alle best practice attuali.	June 28, 2022
Aggiornamento di minore entità	Informazioni aggiuntive su AWS PrivateLink e correzione dei link danneggiati.	May 19, 2022
Aggiornamento di minore entità	Aggiunto AWS PrivateLink.	May 6, 2022
Aggiornamento di minore entità	Rimozione del linguaggio non inclusivo.	April 22, 2022
Aggiornamento di minore entità	Aggiunte informazioni su VPC Network Access Analyzer.	February 2, 2022
Aggiornamento di minore entità	Aggiunta del pilastro della sostenibilità all'introduzione.	December 2, 2021
Aggiornamento di minore entità	Correzione di un link danneggiato.	May 27, 2021
Aggiornamento di minore entità	Modifiche editoriali in varie parti del documento.	May 17, 2021

<u>Aggiornamento principale</u>	Aggiunta una sezione sulla governance, aggiunti dettagli in varie sezioni, aggiunte nuove funzionalità e servizi in tutto il documento.	May 7, 2021
<u>Aggiornamento di minore entità</u>	Link aggiornati.	March 10, 2021
<u>Aggiornamento di minore entità</u>	Correzione di un link danneggiato.	July 15, 2020
<u>Aggiornamenti per il nuovo canone</u>	Linee guida aggiornate sulla gestione di account, identità e autorizzazioni.	July 8, 2020
<u>Aggiornamenti per il nuovo canone</u>	Aggiornato per ampliare i consigli in ogni area, nuove best practice, servizi e funzionalità.	April 30, 2020
<u>Whitepaper aggiornato</u>	Aggiornamenti che rispecchiano i nuovi servizi e le nuove funzionalità di AWS; riferimenti aggiornati.	July 1, 2018
<u>Whitepaper aggiornato</u>	La sezione aggiornata su configurazione e mantenimento della sicurezza del sistema presenta i nuovi servizi e le nuove funzionalità di AWS.	May 1, 2017
<u>Pubblicazione originale</u>	Pubblicazione del Pilastro della sicurezza – Framework AWS Well-Architected.	November 1, 2016

Avvisi

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

© 2021, Amazon Web Services, Inc., o sue affiliate. Tutti i diritti riservati.