Creazione di un programma scalabile di gestione delle vulnerabilità su AWS

AWS Guida prescrittiva

AWS Guida prescrittiva: Creazione di un programma scalabile di gestione delle vulnerabilità su AWS

Table of Contents

Creazione di un programma scalabile di gestione delle vulnerabilità su AWS

Anna McAbee e Megan O'Neil, Amazon Web Services ()AWS

Ottobre 2023 (cronologia del documento)

A seconda della tecnologia di base utilizzata, una varietà di strumenti e scansioni può generare risultati di sicurezza in un ambiente cloud. Senza processi in atto per gestire questi risultati, possono iniziare ad accumularsi, portando spesso a migliaia o decine di migliaia di risultati in un breve lasso di tempo. Tuttavia, con un programma strutturato di gestione delle vulnerabilità e una corretta operatività degli strumenti, l'organizzazione può gestire e valutare un gran numero di risultati provenienti da fonti diverse.

La gestione delle vulnerabilità si concentra sulla scoperta, l'assegnazione delle priorità, la valutazione, la correzione e la segnalazione delle vulnerabilità. La gestione delle patch, d'altra parte, si concentra sull'applicazione di patch o sull'aggiornamento del software per rimuovere o correggere le vulnerabilità di sicurezza. La gestione delle patch è solo un aspetto della gestione delle vulnerabilità. In genere, consigliamo di stabilire sia un patch-in-place processo (noto anche come mitigate-in-placeprocesso) per affrontare scenari critici con applicazione immediata della patch, sia un processo standard da eseguire a cadenza regolare per rilasciare Amazon Machine Images (AMI), contenitori o pacchetti software con patch. Questi processi aiutano a preparare l'organizzazione a rispondere rapidamente a una vulnerabilità zero-day. Per i sistemi critici in un ambiente di produzione, l'utilizzo di un patch-in-place processo può essere più rapido e affidabile rispetto all'implementazione di una nuova AMI in tutta la flotta. Per le patch pianificate regolarmente, come le patch del sistema operativo (OS) e del software, si consiglia di creare e testare utilizzando processi di sviluppo standard, come qualsiasi modifica a livello di software. Ciò offre una migliore stabilità per le modalità operative standard. È possibile utilizzare Patch Manager, una funzionalità di AWS Systems Manager o altri prodotti di terze parti come patch-in-place soluzioni. Per ulteriori informazioni sull'utilizzo di Patch Manager, consulta Gestione delle patch in AWS Cloud Adoption Framework: Operations Perspective. Inoltre, puoi utilizzare EC2 Image Builder per automatizzare la creazione, la gestione e l'implementazione di up-to-date immagini personalizzate e server.

La creazione di un programma scalabile di gestione delle vulnerabilità AWS implica la gestione delle vulnerabilità tradizionali del software e della rete oltre ai rischi di configurazione del cloud. Un rischio legato alla configurazione cloud, ad esempio un bucket Amazon Simple Storage Service (Amazon

S3) non crittografato, dovrebbe seguire un processo di valutazione e correzione simile a quello di una vulnerabilità del software. In entrambi i casi, il team dell'applicazione deve possedere ed essere responsabile della sicurezza della propria applicazione, inclusa l'infrastruttura sottostante. Questa distribuzione della proprietà è fondamentale per un programma di gestione delle vulnerabilità efficace e scalabile.

Questa guida illustra come semplificare l'identificazione e la correzione delle vulnerabilità al fine di ridurre il rischio complessivo. Utilizza le seguenti sezioni per sviluppare e perfezionare il tuo programma di gestione delle vulnerabilità:

1. Preparazione: prepara il personale, i processi e la tecnologia per identificare, valutare e correggere le vulnerabilità nel tuo ambiente.
2. Valutazione e correzione: inoltra i risultati di sicurezza alle parti interessate, identifica l'azione correttiva appropriata e quindi intraprendi l'azione correttiva.
3. Segnala e migliora: utilizza i meccanismi di segnalazione per identificare le opportunità di miglioramento, quindi implementa il tuo programma di gestione delle vulnerabilità.

La creazione di un programma di gestione delle vulnerabilità nel cloud spesso implica un'iterazione. Dai priorità ai consigli contenuti in questa guida e rivedi regolarmente il tuo backlog per rimanere aggiornato sui cambiamenti tecnologici e sui requisiti aziendali.

Destinatari principali

Questa guida è destinata alle grandi aziende che hanno tre team principali responsabili dei risultati relativi alla sicurezza: un team di sicurezza, un Cloud Center of Excellence (CCoE) o team cloud e i team delle applicazioni (o degli sviluppatori). Questa guida utilizza i modelli operativi aziendali più comuni e si basa su tali modelli operativi per consentire una risposta più efficiente ai risultati di sicurezza e migliorare i risultati in materia di sicurezza. Le organizzazioni che utilizzano AWS potrebbero avere strutture e modelli operativi diversi; tuttavia, è possibile modificare molti dei concetti di questa guida per adattarli a modelli operativi diversi e organizzazioni più piccole.

Obiettivi

Questa guida può aiutare te e la tua organizzazione a:

- Sviluppa politiche per semplificare la gestione delle vulnerabilità e garantire la responsabilità

- Stabilisci meccanismi per distribuire la responsabilità della sicurezza ai team applicativi
- Configura in modo pertinente AWS servizi secondo le migliori pratiche per una gestione scalabile delle vulnerabilità
- Distribuisci la proprietà dei risultati di sicurezza
- Stabilisci meccanismi per segnalare e iterare il tuo programma di gestione delle vulnerabilità
- Migliora la visibilità dei risultati di sicurezza e migliora il livello di sicurezza generale

Prepara il tuo programma scalabile di gestione delle vulnerabilità

La preparazione alla creazione di un programma scalabile di gestione delle vulnerabilità implica la formazione delle persone, lo sviluppo di processi e l'implementazione della tecnologia adeguata secondo le migliori pratiche. Le persone, i processi e la tecnologia sono altrettanto importanti per un efficace programma di gestione delle vulnerabilità ed è necessario integrarli strettamente per gestire le vulnerabilità su larga scala.

Questa sezione della guida esamina le azioni fondamentali che è possibile intraprendere per preparare un programma scalabile di gestione delle vulnerabilità. AWS

Argomenti

Definite un piano di gestione delle vulnerabilità

Il primo passo nella preparazione del programma di gestione delle vulnerabilità nel cloud è la definizione del piano di gestione delle vulnerabilità. Questo piano include le politiche e i processi seguiti dall'organizzazione. Questo piano deve essere documentato e accessibile a tutte le parti interessate. Un piano di gestione delle vulnerabilità è un documento di alto livello che in genere include le seguenti sezioni:

- Obiettivi e ambito: delinea gli obiettivi, le funzioni e l'ambito della gestione delle vulnerabilità.
- Ruoli e responsabilità: elenca le parti interessate alla gestione delle vulnerabilità e descrivi le loro responsabilità.
- Definizioni di gravità e prioritizzazione delle vulnerabilità: stabilisci come classificare la gravità di una vulnerabilità e come assegnarle la priorità.

- Accordi sul livello di servizio (SLA) per la correzione: per ogni livello di gravità, definisci il tempo massimo a disposizione del proprietario della soluzione per risolvere un problema di sicurezza. Poiché la conformità agli SLA è parte integrante di un programma di gestione delle vulnerabilità efficace e scalabile, valuta come verificare se stai rispettando questi SLA.
- Processo di eccezione: descrive in dettaglio il processo di invio, approvazione e aggiornamento delle eccezioni. Questo processo dovrebbe garantire che le eccezioni siano legittime, limitate nel tempo e tracciate.
- Fonti di informazioni sulla vulnerabilità: elenca le fonti o gli strumenti che generano risultati di sicurezza. Per ulteriori informazioni su queste AWS servizi che potrebbero essere fonti di rilevazioni di sicurezza, Configura i servizi di sicurezza AWS consulta questa guida.

Sebbene queste sezioni siano comuni a società di diverse dimensioni e settori, il piano di gestione delle vulnerabilità di ogni organizzazione è unico. È necessario creare un piano di gestione delle vulnerabilità che funzioni al meglio per la propria organizzazione. Aspettatevi di modificare il vostro piano nel tempo per incorporare le lezioni apprese e le tecnologie in evoluzione.

Distribuisci la proprietà della sicurezza

Il modello di responsabilitàAWS condivisa definisce in che modo AWS e i suoi clienti condividono la responsabilità per la sicurezza e la conformità del cloud. In questo modello, AWS protegge l'infrastruttura che gestisce tutti i servizi offerti nel e i AWS clienti hanno la Cloud AWS responsabilità di proteggere i propri dati e le proprie applicazioni.

Puoi rispecchiare questo modello all'interno della tua organizzazione e distribuire le responsabilità tra i team che si occupano di cloud e applicazioni. Questo vi aiuta a scalare i vostri programmi di sicurezza cloud in modo più efficace, poiché i team addetti alle applicazioni si assumono la responsabilità di determinati aspetti di sicurezza delle loro applicazioni. L'interpretazione più semplice del modello di responsabilità condivisa è che se si ha accesso per configurare la risorsa, allora si è responsabili della sicurezza di tale risorsa.

Una parte fondamentale della distribuzione delle responsabilità di sicurezza ai team addetti alle applicazioni è la creazione di strumenti di sicurezza self-service che aiutino i team addetti alle applicazioni ad automatizzare. Inizialmente, questo può essere uno sforzo congiunto. Il team addetto alla sicurezza può tradurre i requisiti di sicurezza in strumenti di scansione del codice, quindi i team applicativi possono utilizzare tali strumenti per creare e condividere soluzioni con la propria comunità

di sviluppatori interna. Ciò contribuisce a una maggiore efficienza tra gli altri team che devono soddisfare requisiti di sicurezza simili.

La tabella seguente descrive i passaggi per distribuire la proprietà ai team applicativi e fornisce alcuni esempi.

Fase	Azione	Esempio
1	Definite i vostri requisiti di sicurezza: cosa state cercando di ottenere? Ciò potrebbe derivare da uno standard di sicurezza o da un requisito di conformità.	Un esempio di requisito di sicurezza è l'accesso con privilegi minimi per le identità delle applicazioni.
2	Enumerazione dei controlli per un requisito di sicurezza: cosa significa effettivamente questo requisito dal punto di vista del controllo? Cosa devo fare per raggiungere questo obiettivo?	Per ottenere il minimo privilegi o per le identità delle applicazioni, di seguito sono riportati due controlli di esempio: • Usa i ruoli (IAM) AWS Identity and Access Management • Non utilizzare caratteri jolly nelle policy IAM
3	Guida documentale per i controlli: con questi controlli, quali indicazioni puoi fornire a uno sviluppatore per aiutarlo a rispettare il controllo?	Inizialmente, potresti iniziare documentando semplici policy di esempio, tra cui policy IAM sicure e non sicure e policy bucket di Amazon Simple Storage Service (Amazon S3). Successivamente, puoi incorporare soluzioni di scansione delle policy all'interno di pipeline di integrazione continua e distribuzione

Fase	Azione	Esempio
		continua (CI/CD), ad esempio utilizzando regole per la valutazione proattiva.AWS Config
4	Sviluppa artefatti riutilizzabili: con la guida, puoi renderlo ancora più semplice e sviluppare artefatti riutilizzabili per gli sviluppatori?	Potresti creare un'infrastruttura come codice (IaC) per implementare policy IAM che seguano il principio del privilegio minimo. Puoi archiviare questi artefatti riutilizzabili in un repository di codice.

Il self-service potrebbe non funzionare per tutti i requisiti di sicurezza, ma può funzionare per scenari standard. Seguendo questi passaggi, le organizzazioni possono consentire ai propri team applicativi di gestire un maggior numero di responsabilità in materia di sicurezza in modo scalabile. Nel complesso, il modello di responsabilità distribuita porta a pratiche di sicurezza più collaborative all'interno di molte organizzazioni.

Sviluppa un programma di divulgazione delle vulnerabilità

Per un defense-in-depthapproccio alla gestione delle vulnerabilità, crea un programma di divulgazione delle vulnerabilità in modo che le persone interne o esterne all'organizzazione possano segnalare vulnerabilità o rischi di sicurezza.

Per le persone interne all'organizzazione, stabilisci un processo per segnalare rischi o vulnerabilità. Questo può essere fatto tramite un sistema di ticketing o e-mail. Indipendentemente dal processo scelto, è essenziale che i dipendenti ne siano consapevoli e possano segnalare facilmente eventuali vulnerabilità o rischi che incontrano.

Per le persone esterne all'organizzazione, create una pagina Web esterna per segnalare potenziali vulnerabilità di sicurezza. Ad esempio, consulta la pagina web di segnalazione delle AWS vulnerabilità. Questa pagina web dovrebbe contenere anche linee guida sulla divulgazione per aiutare a proteggere i dati e le risorse dell'organizzazione. Un programma di divulgazione delle

vulnerabilità non dovrebbe incoraggiare attività potenzialmente dannose, quindi è essenziale disporre di una politica chiara con linee guida. Creare un programma di divulgazione maturo e responsabile è un obiettivo da raggiungere man mano che il programma viene sviluppato. La maggior parte non inizia con un programma di divulgazione esterno e ci vuole tempo per farlo bene.

Prepara il tuo ambiente AWS

Prima di implementare qualsiasi strumento di gestione delle vulnerabilità, assicurati che il tuo AWS ambiente sia progettato per supportare un programma scalabile di gestione delle vulnerabilità. La struttura delle politiche di etichettatura proprie Account AWS e della propria organizzazione può semplificare il processo di creazione di un programma scalabile di gestione delle vulnerabilità.

Sviluppa una struttura Account AWS

AWS Organizationsaiuta a gestire e governare centralmente un AWS ambiente man mano che l'azienda cresce e aumenta le AWS risorse. Un'organizzazione in AWS Organizations consolida l'utente Account AWS in gruppi logici o unità organizzative, in modo da poterli amministrare come un'unica unità. È possibile eseguire la gestione AWS Organizations da un account dedicato, denominato account di gestione. Per ulteriori informazioni, consulta Concetti e terminologia di AWS Organizations.

Ti consigliamo di gestire il tuo ambiente AWS con più account in AWS Organizations. Questo aiuta a creare un inventario completo degli account e delle risorse della tua azienda. Questo inventario completo degli asset è un aspetto fondamentale della gestione delle vulnerabilità. I team applicativi non devono utilizzare account esterni all'organizzazione.

AWS Control Towerti aiuta a configurare e gestire un ambiente con AWS più account, seguendo le migliori pratiche prescrittive. Se non hai ancora creato un ambiente con più account, AWS Control Tower è un buon punto di partenza.

Ti consigliamo di utilizzare la struttura di account dedicata e le migliori pratiche descritte nella AWS Security Reference Architecture (AWS SRA). L'account Security Tooling dovrebbe fungere da amministratore delegato per i servizi di sicurezza. Ulteriori informazioni sulla configurazione degli strumenti di gestione delle vulnerabilità in questo account sono fornite più avanti in questa guida. Ospita le applicazioni in account dedicati nell'unità organizzativa (OU) Workloads. Ciò stabilisce un forte isolamento a livello di carico di lavoro e limiti di sicurezza espliciti per ogni applicazione. Per informazioni sui principi di progettazione e sui vantaggi dell'utilizzo di un approccio multi-account, consulta Organizzare l' AWS ambiente utilizzando più account (white paper).AWS

Avere una struttura di account intenzionale e gestire centralmente i servizi di sicurezza da un account dedicato sono aspetti fondamentali di un programma scalabile di gestione delle vulnerabilità.

Definisci, implementa e applica i tag

I tag sono coppie chiave-valore che fungono da metadati per l'organizzazione delle risorse. AWS Per ulteriori informazioni, consulta Tagging delle risorse AWS. È possibile utilizzare i tag per fornire un contesto aziendale, ad esempio l'unità aziendale, il proprietario dell'applicazione, l'ambiente e il centro di costo. La tabella seguente mostra una serie di tag di esempio.

Chiave	Valore
BusinessUnit	HumanResources
CostCenter	CC101
ApplicationTeam	HumanResourcesTechnology
Ambiente	Produzione

I tag possono aiutarti a dare priorità ai risultati. Ad esempio, può aiutarti a:

- Identifica il proprietario di una risorsa responsabile della correzione di una vulnerabilità
- Tieni traccia di quali applicazioni o unità aziendali presentano un gran numero di risultati
- Aumenta la gravità dei risultati per determinate classificazioni di dati, come le informazioni di identificazione personale (PII) o i dati relativi al settore delle carte di pagamento (PCI)
- Identifica il tipo di dati nell'ambiente, ad esempio i dati di test in un ambiente di sviluppo di livello inferiore o i dati di produzione

Per aiutarvi a ottenere un'etichettatura efficace su larga scala, seguite le istruzioni riportate nella sezione Creazione della vostra strategia di tagging in Best Practices for Tagging Resources (white paper AWS).AWS

Monitora i bollettini sulla sicurezza AWS

Consigliamo vivamente di monitorare i bollettini AWS sulla sicurezza su base regolare e frequente. I bollettini sulla sicurezza possono informarti di eventuali nuove vulnerabilità relative alla sicurezza,

dei servizi interessati e degli aggiornamenti applicabili. Puoi anche abbonarti a un feed RSS per i bollettini sulla sicurezza e creare un processo per inserire e gestire questi bollettini come parte del tuo programma di gestione delle vulnerabilità.

Configura i servizi di sicurezza AWS

AWS offre una varietà di servizi di sicurezza progettati per aiutare a proteggere AWS l'ambiente. Per il tuo programma di gestione delle vulnerabilità, ti consigliamo di abilitare quanto segue AWS servizi in ogni account:

- Amazon GuardDuty aiuta a rilevare le minacce attive nel tuo ambiente. Una GuardDuty scoperta potrebbe aiutarti a identificare una vulnerabilità sconosciuta che è stata sfruttata nel tuo ambiente. Potrebbe anche aiutarti a comprendere gli effetti di una vulnerabilità priva di patch.
- AWS Healthoffre una visibilità continua sulle prestazioni delle risorse e sulla disponibilità degli account e degli account AWS servizi .
- AWS Identity and Access Management Access Analyzeranalizza le politiche basate sulle risorse nell' AWS ambiente per identificare le risorse condivise con un'entità esterna. Questo può aiutarti a identificare le vulnerabilità associate all'accesso involontario alle tue risorse e ai tuoi dati. Per ogni istanza di una risorsa condivisa al di fuori dell'account, Sistema di analisi degli accessi AWS IAM genera un risultato.
- Amazon Inspector è un servizio di gestione delle vulnerabilità che analizza continuamente i AWS carichi di lavoro alla ricerca di vulnerabilità del software ed esposizione involontaria della rete.
- AWS Security Hubti aiuta a controllare il tuo AWS ambiente rispetto agli standard del settore della sicurezza e a identificare i rischi legati alla configurazione del cloud. Fornisce inoltre una visione completa dello stato di AWS sicurezza aggregando i risultati di altri servizi di AWS sicurezza e strumenti di sicurezza di terze parti.

Questa sezione spiega come abilitare e configurare Amazon Inspector e Security Hub per aiutarti a stabilire un programma scalabile di gestione delle vulnerabilità.

Utilizzo di Amazon Inspector nel programma di gestione delle vulnerabilità

Amazon Inspector è un servizio di gestione delle vulnerabilità che analizza continuamente le istanze e le funzioni dei container Amazon Elastic Compute Cloud (Amazon EC2), le immagini dei container Amazon Elastic Container Registry (Amazon ECR) e le funzioni per individuare le vulnerabilità del

software e l'esposizione involontaria della rete. AWS Lambda Puoi usare Amazon Inspector per ottenere visibilità e dare priorità alla risoluzione delle vulnerabilità del software nei tuoi ambienti. AWS

Amazon Inspector valuta continuamente il tuo ambiente durante l'intero ciclo di vita delle tue risorse. Esegue automaticamente una nuova scansione delle risorse in risposta a modifiche che potrebbero introdurre una nuova vulnerabilità. Ad esempio, esegue nuovamente la scansione quando si installa un nuovo pacchetto su un'istanza EC2, quando si installa una patch o quando viene pubblicata una nuova vulnerabilità ed esposizione comune (CVE) che influisce sulla risorsa. Quando Amazon Inspector identifica una vulnerabilità o un percorso di rete aperto, produce un risultato che puoi esaminare. La scoperta fornisce informazioni complete sulla vulnerabilità, tra cui:

- Punteggio di rischio di Amazon Inspector
- Punteggio CVSS (Common Vulnerability Scoring System)
- Risorsa interessata
- dati di intelligence sulle vulnerabilità relativi al CVE forniti da Amazon e Recorded FutureCybersecurity and Infrastructure Security Agency (CISA)
- Raccomandazioni per la riparazione

Per istruzioni sulla configurazione di Amazon Inspector, consulta la sezione Guida introduttiva ad Amazon Inspector. Il passaggio Activate Amazon Inspector di questo tutorial offre due opzioni di configurazione: un ambiente di account autonomo e un ambiente multi-account. Ti consigliamo di utilizzare l'opzione di ambiente multi-account se desideri monitorare più Account AWS membri di un'organizzazione in. AWS Organizations

Quando configuri Amazon Inspector per un ambiente con più account, definisci un account dell'organizzazione come amministratore delegato di Amazon Inspector. L'amministratore delegato può gestire i risultati e alcune impostazioni per i membri dell'organizzazione. Ad esempio, l'amministratore delegato può visualizzare i dettagli dei risultati aggregati per tutti gli account dei membri, abilitare o disabilitare le scansioni degli account dei membri e rivedere le risorse analizzate. L' AWS SRA consiglia di creare un account Security Tooling e di utilizzarlo come amministratore delegato di Amazon Inspector.

Utilizzabile AWS Security Hub nel tuo programma di gestione delle vulnerabilità

La creazione di un programma scalabile di gestione delle vulnerabilità AWS implica la gestione delle vulnerabilità tradizionali del software e della rete oltre ai rischi di configurazione del cloud. AWS Security Hubti aiuta a controllare il tuo AWS ambiente rispetto agli standard del settore della sicurezza e a identificare i rischi legati alla configurazione del cloud. Security Hub fornisce anche una visione completa dello stato di sicurezza AWS aggregando i risultati di sicurezza di altri servizi di AWS sicurezza e strumenti di sicurezza di terze parti.

Nelle seguenti sezioni, forniamo le migliori pratiche e consigli per configurare Security Hub a supporto del tuo programma di gestione delle vulnerabilità:

- Configurazione del Security Hub
- Abilitazione degli standard Security Hub
- Gestione dei risultati del Security Hub
- Aggregazione dei risultati di altri servizi e strumenti di sicurezza

Configurazione del Security Hub

Per le istruzioni di configurazione, vedere Configurazione AWS Security Hub. Per utilizzare Security Hub, è necessario abilitare AWS Config. Per ulteriori informazioni, vedere Abilitazione e configurazione AWS Config nella documentazione del Security Hub.

Se si è integrati con AWS Organizations, dall'account di gestione dell'organizzazione, si designa un account come amministratore delegato del Security Hub. Per istruzioni, vedere Designazione dell'amministratore delegato del Security Hub. L' AWS SRA consiglia di creare un account Security Tooling e di utilizzarlo come amministratore delegato del Security Hub.

L'amministratore delegato ha automaticamente accesso alla configurazione del Security Hub per tutti gli account dei membri dell'organizzazione e alla visualizzazione dei risultati associati a tali account. Ti consigliamo di abilitare AWS Config Security Hub in tutti Regioni AWS i tuoi Account AWS. È possibile configurare Security Hub per trattare automaticamente i nuovi account dell'organizzazione come account membri di Security Hub. Per istruzioni, consulta Gestione degli account dei membri che appartengono a un'organizzazione.

Abilitazione degli standard Security Hub

Security Hub genera risultati eseguendo controlli di sicurezza automatici e continui rispetto ai controlli di sicurezza. I controlli sono associati a uno o più standard di sicurezza. I controlli consentono di determinare se i requisiti di uno standard sono soddisfatti.

Quando abiliti uno standard in Security Hub, Security Hub abilita automaticamente i controlli che si applicano allo standard. Security Hub utilizza AWS Config regole per eseguire la maggior parte dei controlli di sicurezza. Puoi abilitare o disabilitare gli standard Security Hub in qualsiasi momento. Per ulteriori informazioni, consulta Controlli e standard di sicurezza in AWS Security Hub. Per un elenco completo degli standard, consulta il riferimento agli standard di Security Hub.

Se la tua organizzazione non dispone già di uno standard di sicurezza preferito, ti consigliamo di utilizzare lo standard AWS Foundational Security Best Practices (FSBP). Questo standard è progettato per rilevare quando Account AWS e quali risorse si discostano dalle migliori pratiche di sicurezza. AWS cura questo standard e lo aggiorna regolarmente per includere nuove funzionalità e servizi. Dopo aver esaminato i risultati del FSBP, valuta la possibilità di abilitare altri standard.

Gestione dei risultati del Security Hub

Security Hub offre diverse funzionalità che aiutano a gestire grandi volumi di risultati provenienti da tutta l'organizzazione e a comprendere lo stato di sicurezza del proprio AWS ambiente. Per aiutarti a gestire i risultati, ti consigliamo di abilitare le seguenti due funzionalità di Security Hub:

- Utilizza l'aggregazione tra aree geografiche per aggregare i risultati, trovare aggiornamenti, approfondimenti, controllare gli stati di conformità e i punteggi di sicurezza da più aree di aggregazione Regioni AWS a una singola.
- Utilizza i risultati di controllo consolidati per ridurre i problemi di ricerca rimuovendo i risultati duplicati. Quando i risultati del controllo consolidato sono attivati nel tuo account, Security Hub genera un singolo nuovo risultato o aggiornamento dei risultati per ogni controllo di sicurezza di un controllo, anche se un controllo si applica a più standard abilitati.

Aggregazione dei risultati di altri servizi e strumenti di sicurezza

Oltre a generare risultati di sicurezza, puoi utilizzare Security Hub per aggregare i dati dei risultati provenienti da diverse AWS servizi soluzioni di sicurezza di terze parti supportate. Questa sezione si concentra sull'invio dei risultati di sicurezza a Security Hub. La sezione successiva illustra come

integrare Security Hub con prodotti in grado di ricevere risultati da Security Hub. Preparati ad assegnare i risultati di sicurezza

Sono disponibili molti AWS servizi prodotti di terze parti e soluzioni open source che puoi integrare con Security Hub. Se hai appena iniziato, ti consigliamo di fare quanto segue:

1. Abilita integrazione AWS servizi: la maggior parte delle AWS servizio integrazioni che inviano i risultati a Security Hub vengono attivate automaticamente dopo aver abilitato sia Security Hub che il servizio integrato. Per il tuo programma di gestione delle vulnerabilità, ti consigliamo di abilitare Amazon Inspector AWS Health, GuardDuty Amazon e IAM Access Analyzer in ogni account. Questi servizi inviano automaticamente i risultati a Security Hub. Per un elenco completo delle AWS servizio integrazioni supportate, vedi AWS servizi che invia i risultati a Security Hub.

   > **Note**
   >
   > AWS Health invia i risultati a Security Hub se viene soddisfatta una delle seguenti condizioni:
   >
   > - Il risultato è associato a un servizio AWS di sicurezza
   > - Il codice tipo di ricerca contiene le parole `securityabuse`, o `certificate`
   > - Il AWS Health servizio di ricerca è `risk` o `abuse`

2. Configurare integrazioni di terze parti: per un elenco delle integrazioni attualmente supportate, consulta Integrazioni di prodotti di partner di terze parti disponibili. Seleziona eventuali strumenti aggiuntivi in grado di inviare o ricevere risultati da Security Hub. Potresti già disporre di alcuni di questi strumenti di terze parti. Segui le istruzioni del prodotto per configurare l'integrazione con Security Hub.

Preparati ad assegnare i risultati di sicurezza

In questa sezione, configuri gli strumenti che i tuoi team utilizzano per gestire e assegnare i risultati di sicurezza. Questa sezione include le seguenti opzioni:

- Gestisci i risultati negli strumenti e nei flussi di lavoro esistenti— Questa opzione si integra AWS Security Hub con i sistemi esistenti utilizzati dai team per gestire le attività quotidiane, come il backlog dei prodotti. Questa opzione è consigliata per i team che dispongono di strumenti per gestire i propri flussi di lavoro.

- Gestisci i risultati in Security Hub— Questa opzione configura le notifiche per gli eventi del Security Hub in modo che il team appropriato riceva un avviso e possa risolvere il problema in Security Hub.

Decidi quale flusso di lavoro è più adatto ai tuoi team e assicurati che i risultati relativi alla sicurezza possano essere trasmessi tempestivamente ai rispettivi proprietari.

Gestisci i risultati negli strumenti e nei flussi di lavoro esistenti

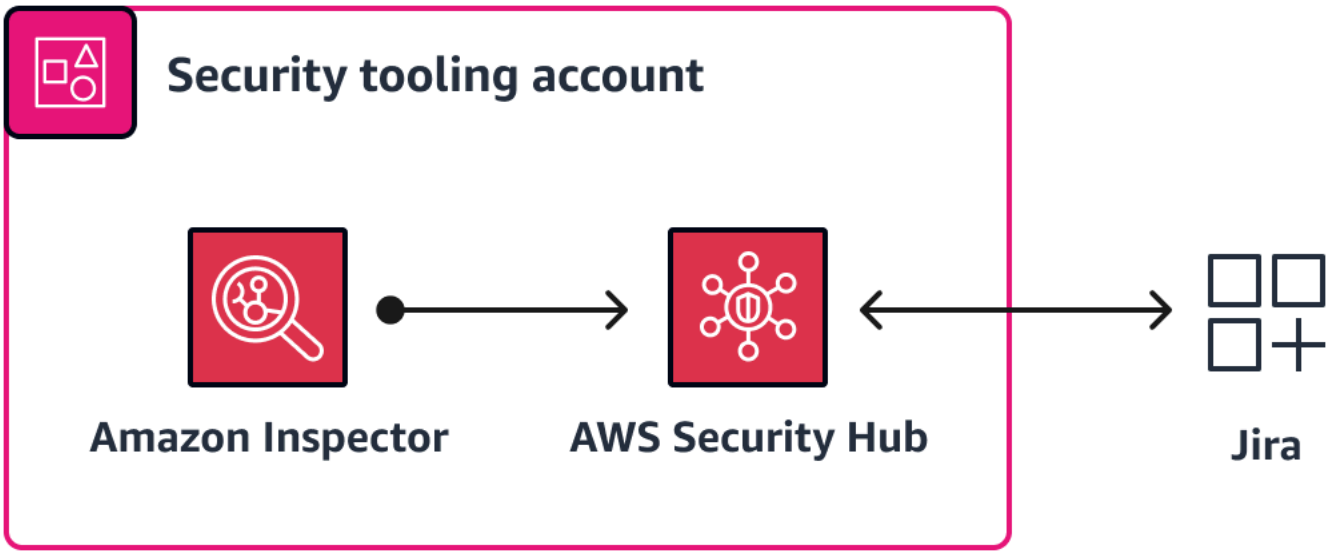
Consigliamo integrazioni aggiuntive di Security Hub per le organizzazioni aziendali che dispongono di strumenti consolidati che i team utilizzano per gestire o svolgere le proprie attività quotidiane. È possibile importare i dati di ricerca di Security Hub in diverse piattaforme tecnologiche. Esempi includono:

- I sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM) aiutano i team di sicurezza a valutare gli eventi di sicurezza operativi. I sistemi SIEM forniscono un'analisi in tempo reale degli avvisi di sicurezza generati dalle applicazioni e dall'hardware di rete.
- I sistemi di governance, rischio e conformità (GRC) aiutano i team di conformità e governance a monitorare e riferire sui dati di gestione del rischio. Gli strumenti GRC sono applicazioni software che le aziende possono utilizzare per gestire le politiche, valutare i rischi, controllare l'accesso degli utenti e semplificare la conformità. È possibile utilizzare gli strumenti GRC per integrare i processi aziendali, ridurre i costi e migliorare l'efficienza.
- I sistemi di product backlog e ticketing aiutano i team addetti alle applicazioni e al cloud a gestire le funzionalità e a dare priorità alle attività di sviluppo. Atlassian Jirae Microsoft Azure DevOpssono esempi di questi sistemi.

L'integrazione dei risultati del Security Hub direttamente con questi sistemi aziendali esistenti può migliorare il tempo medio di ripristino (MTTR) e i risultati di sicurezza, perché il flusso di lavoro operativo quotidiano non deve cambiare. I team possono rispondere e imparare dai risultati della sicurezza molto più velocemente perché non devono utilizzare flussi di lavoro e strumenti separati. L'integrazione rende la risoluzione dei problemi di sicurezza parte del normale flusso di lavoro standard.

Security Hub si integra con diversi prodotti partner di terze parti. Per un elenco completo e le istruzioni, consulta Integrazioni di prodotti di partner di terze parti disponibili nella documentazione di Security Hub. Le integrazioni più comuni includono Atlassian - Jira Service Managementl'integrazione bidirezionale AWS Security Hub con Jira il software e. ServiceNow – ITSM Il diagramma seguente

mostra come configurare Amazon Inspector per inviare i risultati a Security Hub e quindi configurare Security Hub a cui inviare tutti i risultati. Jira



Gestisci i risultati in Security Hub

Puoi creare un sistema di notifica basato sul cloud per i risultati del Security Hub utilizzando EventBridge le regole di Amazon e gli argomenti di Amazon Simple Notification Service (Amazon SNS). Questo sistema notifica al team appropriato una scoperta al momento della creazione. Per questo approccio, la strategia multi-account descritta in Sviluppa una struttura Account AWS è fondamentale perché le applicazioni sono separate in account dedicati. Questo ti aiuta a notificare ai team corretti ogni risultato.

I team addetti alla sicurezza o al cloud potrebbero scegliere di ricevere eventi da tutti Account AWS. In questo caso, crea una EventBridge regola all'interno dell'account amministratore delegato di Security Hub e iscriviti a un argomento Amazon SNS per informare questi team. Per i team applicativi, configura una EventBridge regola e un argomento SNS all'interno dei rispettivi account applicativi. Quando si verifica un rilevamento del Security Hub all'interno di un account dell'applicazione, il team responsabile riceve una notifica del risultato.

Security Hub invia già automaticamente tutti i nuovi risultati e tutti gli aggiornamenti dei risultati esistenti EventBridge come Security Hub Findings - Imported events. Ogni evento Security Hub Findings - Imported contiene un singolo risultato. È possibile applicare filtri alle EventBridge regole in modo che un risultato avvii la regola solo se il risultato corrisponde ai filtri. Per istruzioni, vedi Configurazione di una EventBridge regola per l'invio automatico dei risultati. Per ulteriori informazioni

sulla creazione e l'iscrizione agli argomenti di Amazon SNS, consulta Configurazione di Amazon SNS.

Quando utilizzi questo approccio, considera quanto segue:

- Per i team addetti alle applicazioni, create EventBridge regole all'interno di ciascun Account AWS Regione AWS luogo in cui è ospitata l'applicazione.
- Per i team addetti alla sicurezza e al cloud, crea EventBridge regole nell'account amministratore delegato di Security Hub. In questo modo i team vengono notificati tutti i risultati negli account dei membri.
- Amazon SNS invia una notifica ogni giorno se lo stato del risultato di sicurezza è lo stesso. `NEW` Se desideri disattivare le notifiche giornaliere, puoi creare una AWS Lambda funzione personalizzata che modifica lo stato della ricerca da `NEW` a `NOTIFIED` dopo che l'abbonato Amazon SNS ha ricevuto la notifica.

Valuta e correggi i problemi di sicurezza nel tuo ambiente AWS

La valutazione di un problema di sicurezza implica l'inoltro del risultato allo stakeholder appropriato, la valutazione e l'assegnazione delle priorità al risultato, quindi la correzione. Questa sezione esamina in dettaglio ciascuno di questi passaggi e fornisce consigli per la scalabilità e l'efficienza. Include anche esempi che aiutano a illustrare il processo di valutazione e riparazione.

Argomenti

Definisci la titolarità dei risultati di sicurezza

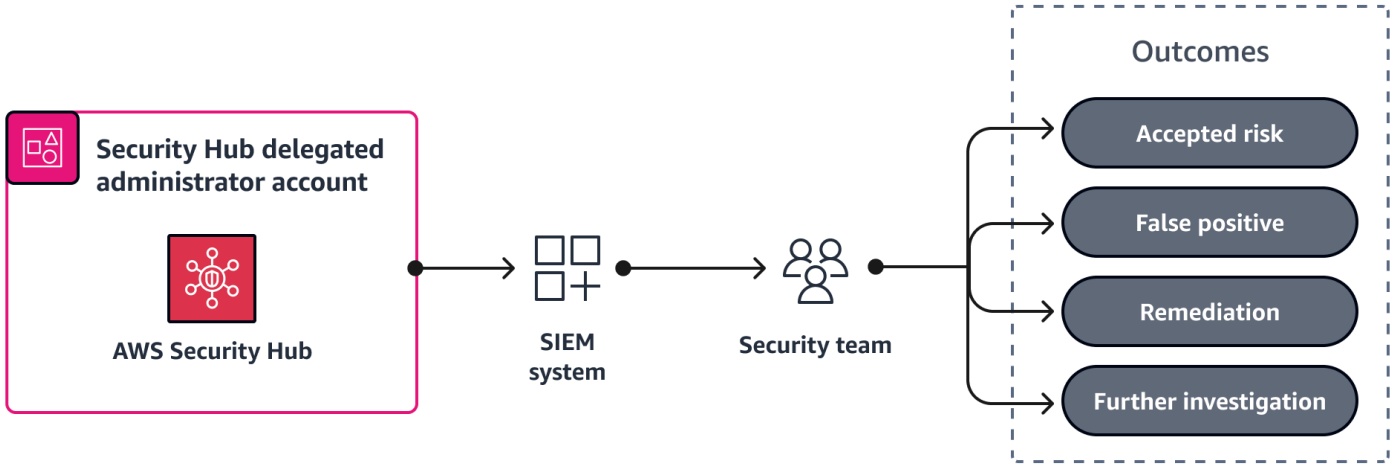
Definire un modello di proprietà per valutare i risultati in materia di sicurezza può essere difficile, ma non deve esserlo necessariamente. Il panorama della sicurezza cambia costantemente e gli operatori devono essere flessibili per adattarsi a questi cambiamenti. Adotta un approccio flessibile per sviluppare il tuo modello di proprietà ai fini della sicurezza. Il modello iniziale dovrebbe consentire ai team di agire immediatamente. Ti consigliamo di iniziare con una logica di proprietà di base e di perfezionarla nel tempo. Se si ritarda a definire i criteri di proprietà perfetti, il numero di risultati di sicurezza continuerà a crescere.

Per facilitare l'assegnazione dei risultati ai team e alle risorse appropriati, consigliamo l'integrazione AWS Security Hub con tutti i sistemi esistenti utilizzati dai team per gestire le attività quotidiane. Ad esempio, puoi integrare Security Hub con i sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM) o i sistemi di backlog e ticketing dei prodotti. Per ulteriori informazioni sul tagging, consulta Preparati ad assegnare i risultati di sicurezzain questa guida.

Di seguito è riportato un esempio di modello di proprietà che è possibile utilizzare come punto di partenza:

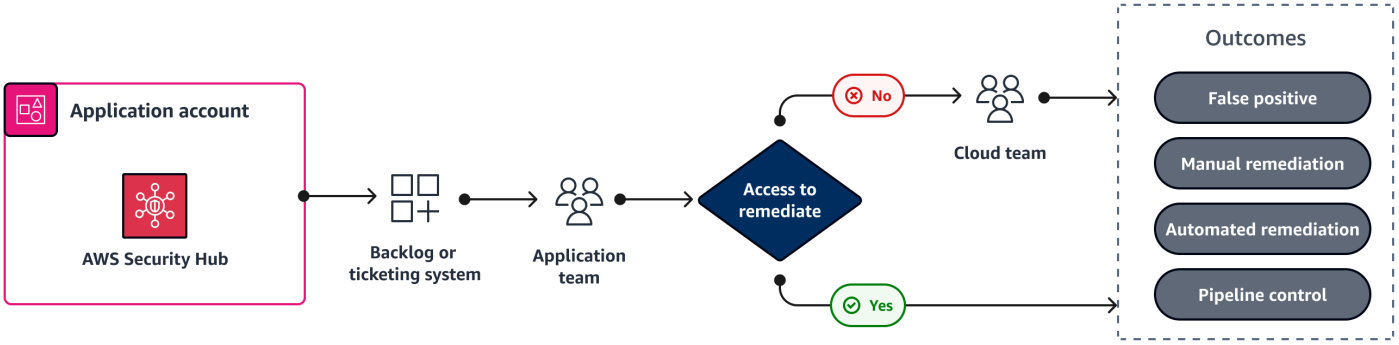
- Il team addetto alla sicurezza esamina le minacce potenzialmente attive e aiuta a valutare e dare priorità ai risultati di sicurezza. Il team addetto alla sicurezza dispone delle competenze e degli

strumenti per valutare correttamente il contesto. Conoscono i dati aggiuntivi relativi alla sicurezza che li aiutano a valutare e dare priorità alle vulnerabilità e a indagare sugli eventi di rilevamento delle minacce. Se è necessario determinare la gravità o eseguire ulteriori regolazioni, consulta la sezione di questa guida. Valuta e dai priorità ai risultati di sicurezza Per un esempio, Esempio di team di sicurezza consulta questa guida.



- Distribuisci i risultati di sicurezza tra i team del cloud e quelli delle applicazioni: come illustrato nella Distribuisci la proprietà della sicurezza sezione, il team che ha accesso alla configurazione della risorsa è responsabile della sua configurazione sicura. I team applicativi sono responsabili dei risultati di sicurezza relativi alle risorse che creano e configurano, mentre il team cloud è responsabile dei risultati di sicurezza relativi alle configurazioni di ampia portata. Nella maggior parte dei casi, i team applicativi non hanno accesso a modificare configurazioni di ampia portata e AWS servizi, ad esempio, le policy di controllo dei servizi (SCP) AWS Control Tower, le configurazioni VPC AWS Organizations relative alla rete e IAM Identity Center.AWS

  Per gli ambienti con più account che separano le applicazioni in account dedicati, in genere è possibile integrare i risultati relativi alla sicurezza dell'account nel backlog o nel sistema di ticketing dell'applicazione. Da quel sistema, il team cloud o il team applicativo possono risolvere il problema. Per esempi, vedi Esempio di team cloud o Esempio di team applicativo in questa guida.



- Assegna i risultati rimanenti e irrisolti al team cloud: i risultati residui potrebbero essere correlati alle impostazioni predefinite o a configurazioni di ampia portata che il team cloud può gestire. Questo team ha probabilmente le conoscenze e l'accesso più approfonditi sulla storia per risolvere il problema. Nel complesso, si tratta in genere di un sottoinsieme significativamente più piccolo dei risultati totali.

Valuta e dai priorità ai risultati di sicurezza

Un componente fondamentale di un efficace programma di gestione delle vulnerabilità è la capacità di valutare e dare priorità ai risultati di sicurezza. È qui che entrano in gioco il contesto, la cronologia organizzativa e l'ottimizzazione dei sistemi di rilevamento. L'assegnazione di priorità ai risultati di sicurezza aiuta a stabilire la velocità appropriata per il livello di risposta.

Per Amazon Inspector e Amazon AWS Security Hub GuardDuty, i risultati contengono un'etichetta o un punteggio di gravità. Consigliamo di dare priorità all'analisi di tutti i risultati critici e di elevata gravità in Security Hub, compresi i risultati relativi allo standard Foundational Security Best Practices (FSBP), Amazon Inspector e. GuardDuty I punteggi delle etichette di gravità dei risultati sono determinati come segue:

- Il punteggio Amazon Inspector è un punteggio altamente contestualizzato per ogni risultato. Viene calcolato correlando le informazioni sul punteggio di base del Common Vulnerability Scoring System (CVSS) con i risultati di raggiungibilità della rete e i dati di sfruttabilità. Utilizzando questo punteggio, puoi dare priorità ai risultati per concentrarti sui risultati più critici e sulle risorse più vulnerabili. Oltre al punteggio, Amazon Inspector fornisce anche informazioni avanzate sulle vulnerabilità relative a Common Vulnerabilities and Exposures (CVE). Questo è un riepilogo delle informazioni disponibili sul CVE di Amazon e di fonti di intelligence sulla sicurezza standard del settore, come Recorded Future e Cybersecurity and Infrastructure Security Agency (CISA). Ad

esempio, Amazon Inspector può fornire i nomi di kit di malware noti utilizzati per sfruttare una vulnerabilità. Per ulteriori informazioni, consulta Vulnerability Intelligence.

- A ogni GuardDuty risultato è assegnato un livello di gravità e un valore che riflettono il rischio potenziale del risultato per l'ambiente in uso. Questo livello e valore sono determinati dai tecnici AWS della sicurezza. Ad esempio, un livello di `High` gravità indica che una risorsa è compromessa e viene utilizzata attivamente per scopi non autorizzati. Si consiglia di considerare prioritario l' GuardDuty accertamento `High` della gravità e di porvi immediatamente rimedio per evitare ulteriori utilizzi non autorizzati.
- La gravità di un risultato di controllo del Security Hub è determinata dalla difficoltà da sfruttare e dalla probabilità di compromissione. La difficoltà è determinata dal livello di sofisticazione o complessità necessario per utilizzare la vulnerabilità per realizzare uno scenario di minaccia. La probabilità di compromissione indica la probabilità che lo scenario di minaccia comporti un'interruzione o una violazione delle risorse o delle risorse. AWS servizi

Per ottimizzare i risultati, puoi sopprimere o archiviare risultati specifici direttamente nella rispettiva console di servizio o utilizzando l'API del servizio. Inoltre, puoi apportare modifiche ai risultati in Security Hub utilizzando le regole di automazione. GuardDuty e i risultati di Amazon Inspector vengono inviati automaticamente a Security Hub. Puoi utilizzare le regole di automazione per aggiornare automaticamente (ad esempio modificando la gravità) o eliminare i risultati quasi in tempo reale, in base a criteri definiti da te. Quando crei le regole di automazione, ti consigliamo di aggiungere un contesto alla descrizione della regola, ad esempio la data di creazione o modifica, chi l'ha creata e il motivo per cui la regola è necessaria. Queste informazioni sono spesso utili per riferimenti futuri.

Correggi i problemi di sicurezza

Dopo aver valutato e dato priorità a un risultato, l'azione successiva consiste nel porvi rimedio. Esistono molte azioni diverse che è possibile intraprendere per correggere un risultato. Per le vulnerabilità del software, è possibile aggiornare il sistema operativo o applicare una patch. Per i risultati della configurazione cloud, puoi aggiornare la configurazione delle risorse. In generale, le azioni intraprese per porre rimedio possono essere raggruppate in uno dei seguenti risultati:

- Correzione manuale: si fornisce manualmente una correzione alla vulnerabilità, ad esempio modificando le proprietà di una risorsa per abilitare la crittografia. AWS Se il risultato proviene da un controllo gestito in Security Hub, il risultato include un collegamento alle istruzioni per correggere manualmente il risultato.

- Artefatto riutilizzabile: aggiorni l'infrastruttura come codice (IaC) per correggere la vulnerabilità e sapere che altri potrebbero trarre vantaggio da una soluzione simile. Valuta la possibilità di caricare l'IaC aggiornato e un breve riepilogo della risoluzione in un repository di codice condiviso interno.
- Riparazione automatica: la vulnerabilità viene risolta automaticamente tramite meccanismi creati dall'utente.
- Controllo della pipeline: applichi un controllo all'interno della pipeline di integrazione continua e distribuzione continua (CI/CD) che impedisce l'implementazione se la vulnerabilità è presente.
- Rischio accettato: non intraprendete alcuna azione o implementate un controllo compensativo e accettate il rischio rappresentato dalla vulnerabilità. Tieni traccia del rischio accettato in una posizione dedicata, ad esempio un registro dei rischi.
- Falso positivo: non intraprendi alcuna azione perché hai stabilito che la scoperta non ha identificato correttamente una vulnerabilità.

Un elenco completo delle varie azioni che è possibile intraprendere e degli strumenti che è possibile utilizzare per correggere una vulnerabilità non rientra nell'ambito di questa guida. Tuttavia, vi sono alcuni servizi e strumenti che possono aiutarvi a correggere vulnerabilità su larga scala che vale la pena notare, tra cui:

- Patch Manager, una funzionalità di AWS Systems Manager, automatizza il processo di applicazione di patch ai nodi gestiti con aggiornamenti relativi alla sicurezza e altri tipi di aggiornamenti. Gestione patch consente di applicare patch sia per i sistemi operativi sia per le applicazioni
- AWS Firewall Managerti aiuta a configurare e gestire centralmente le regole del firewall tra i tuoi account e le tue applicazioni in. AWS Organizations Man mano che vengono create nuove applicazioni, Firewall Manager semplifica la conformità di nuove applicazioni e risorse applicando un set comune di regole di sicurezza.
- Automated Security Response on AWS è una AWS soluzione che funziona con Security Hub e fornisce azioni di risposta e riparazione predefinite basate sugli standard di conformità del settore e sulle migliori pratiche per le minacce alla sicurezza.

Esempi di valutazione e correzione dei risultati di sicurezza

Questa sezione fornisce esempi del processo di triage per i team addetti alla sicurezza, al cloud e alle applicazioni. Descrive i tipi di risultati che ogni team affronta comunemente e fornisce un esempio di come rispondere. Sono incluse anche linee guida di alto livello per la correzione.

In questa sezione sono inclusi gli esempi seguenti:

- Esempio di team di sicurezza: creazione di una regola di automazione Security Hub
- Esempio di team cloud: modifica delle configurazioni VPC
- Esempio di team applicativo: creazione di una regola AWS Config

Esempio di team di sicurezza: creazione di una regola di automazione Security Hub

Il team di sicurezza riceve i risultati relativi al rilevamento delle minacce, inclusi GuardDuty i risultati di Amazon. Per un elenco completo dei tipi di GuardDuty ricerca classificati per tipo di AWS risorsa, consulta Finding types nella GuardDuty documentazione. I team addetti alla sicurezza devono conoscere tutti questi tipi di risultati.

Per questo esempio, il team addetto alla sicurezza accetta il livello di rischio associato ai risultati di sicurezza in un documento Account AWS che viene utilizzato esclusivamente per scopi di apprendimento e non include dati importanti o sensibili. Il nome di questo account è`sandbox`, e l'ID dell'account è`123456789012`. Il team addetto alla sicurezza può creare una regola di AWS Security Hub automazione che sopprime tutti i GuardDuty risultati di questo account. Possono creare una regola da un modello, che copre molti casi d'uso comuni, oppure creare una regola personalizzata. In Security Hub, consigliamo di visualizzare in anteprima i risultati dei criteri per confermare che la regola restituisca i risultati previsti.

> **Note**
>
> Questo esempio evidenzia la funzionalità delle regole di automazione. Non è consigliabile eliminare tutti i GuardDuty risultati relativi a un account. Il contesto è importante e ogni organizzazione deve scegliere quali risultati eliminare in base al tipo di dati, alla classificazione e ai controlli di mitigazione.

Di seguito sono riportati i parametri utilizzati per creare questa regola di automazione:

- Regola:
  - Il nome della regola è `Suppress findings from Sandbox account`
  - La descrizione della regola è `Date: 06/25/23 Authored by: John Doe Reason: Suppress GuardDuty findings from the sandbox account`

- Criteri:
  - `AwsAccountId` = `123456789012`
  - `ProductName` = `GuardDuty`
  - `WorkflowStatus` = `NEW`
  - `RecordState` = `ACTIVE`
- Azione automatizzata:
  - `Workflow.status` è `SUPPRESSED`

Per ulteriori informazioni, consulta Regole di automazione nella documentazione del Security Hub. I team di sicurezza hanno a disposizione molte opzioni per indagare e correggere i risultati delle minacce rilevate. Per una guida completa, consulta la AWS Security Incident Response Guide. Ti consigliamo di consultare questa guida per confermare di aver stabilito solidi processi di risposta agli incidenti.

Esempio di team cloud: modifica delle configurazioni VPC

Il team cloud è responsabile della valutazione e della correzione dei risultati di sicurezza che presentano tendenze comuni, come le modifiche alle impostazioni AWS predefinite che potrebbero non essere adatte al caso d'uso. Questi risultati tendono a influire su molte Account AWS risorse, come le configurazioni VPC, oppure includono una restrizione che deve essere applicata all'intero ambiente. Per la maggior parte, il team cloud apporta modifiche manuali una tantum, come l'aggiunta o l'aggiornamento di una policy.

Dopo che l'organizzazione ha utilizzato un AWS ambiente per qualche tempo, è possibile che si stia sviluppando una serie di anti-pattern. Un anti-pattern è una soluzione utilizzata frequentemente per un problema ricorrente in cui la soluzione è controproducente, inefficace o meno efficace di un'alternativa. In alternativa a questi anti-pattern, l'organizzazione può utilizzare restrizioni a livello di ambiente più efficaci, come le policy di controllo dei AWS Organizations servizi (SCP) o i set di autorizzazioni di IAM Identity Center. Gli SCP e i set di autorizzazioni possono fornire restrizioni aggiuntive per i tipi di risorse, ad esempio impedire agli utenti di configurare un bucket Amazon Simple Storage Service (Amazon S3) pubblico. Sebbene si possa essere tentati di limitare ogni possibile configurazione di sicurezza, esistono dei limiti di dimensione delle policy per gli SCP e i set di autorizzazioni. Consigliamo un approccio equilibrato ai controlli preventivi e investigativi.

Di seguito sono riportati alcuni controlli dello standard AWS Security Hub Foundational Security Best Practices (FSBP) di cui il team cloud potrebbe essere responsabile:

- [EC2.2] Il gruppo di sicurezza predefinito VPC non dovrebbe consentire il traffico in entrata e in uscita
- [EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC
- [EC2.23] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC
- [CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura
- [Config.1] AWS Config dovrebbe essere abilitato

Per questo esempio, il team cloud sta esaminando una scoperta relativa al controllo FSBP EC2.2. La documentazione relativa a questo controllo consiglia di non utilizzare il gruppo di sicurezza predefinito perché consente un ampio accesso tramite le regole predefinite in entrata e in uscita. Poiché il gruppo di sicurezza predefinito non può essere eliminato, si consiglia di modificare le impostazioni delle regole per limitare il traffico in entrata e in uscita. Per risolvere efficacemente questo problema, il team cloud dovrebbe utilizzare meccanismi consolidati per modificare le regole dei gruppi di sicurezza per tutti i VPC, poiché ogni VPC ha questo gruppo di sicurezza predefinito. Nella maggior parte dei casi, i team cloud gestiscono le configurazioni VPC utilizzando AWS Control Towerpersonalizzazioni o uno strumento Infrastructure as Code (IaC), come o. HashiCorp TerraformAWS CloudFormation

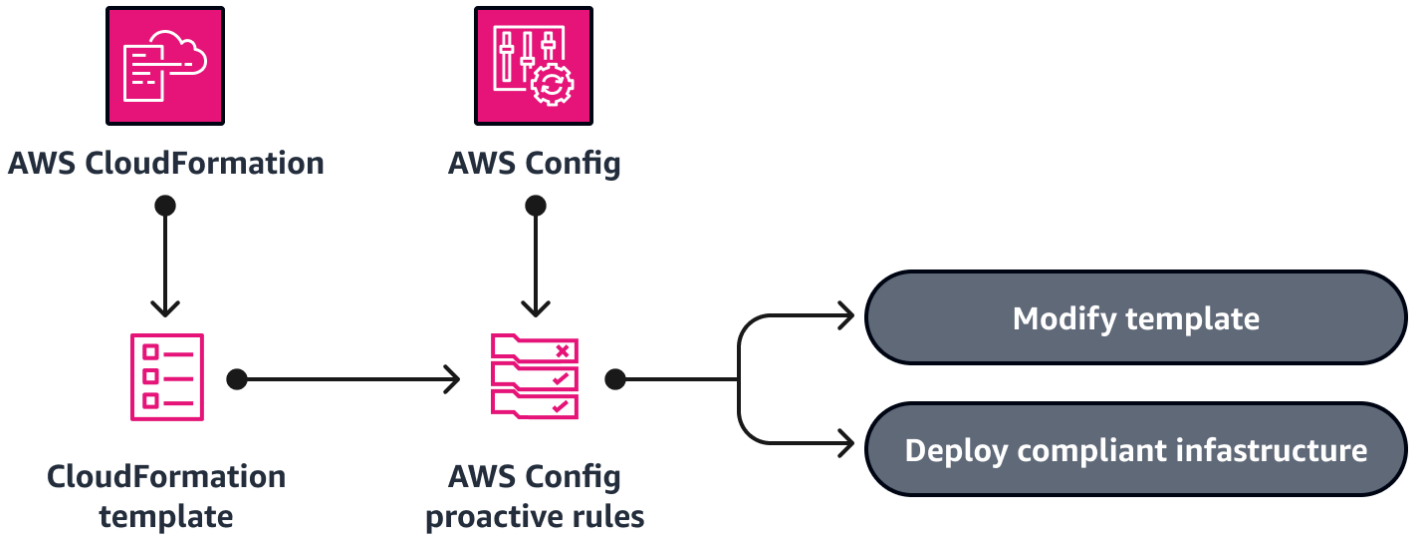
Esempio di team applicativo: creazione di una regola AWS Config

Di seguito sono riportati alcuni controlli dello standard di sicurezza Security Hub Foundational Security Best Practices (FSBP) di cui l'applicazione o il team di sviluppo potrebbero essere responsabili:

- [CloudFront.1] le CloudFront distribuzioni devono avere un oggetto root predefinito configurato
- [EC2.19] I gruppi di sicurezza non dovrebbero consentire l'accesso illimitato alle porte ad alto rischio
- [CodeBuild.1] CodeBuild GitHub o gli URL del repository di origine Bitbucket devono utilizzare OAuth
- [ECS.4] I contenitori ECS devono essere eseguiti come non privilegiati
- [ELB.1] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS

Per questo esempio, il team dell'applicazione sta esaminando una scoperta relativa al controllo FSBP EC2.19. Questo controllo verifica se il traffico in entrata senza restrizioni per i gruppi di sicurezza è accessibile alle porte specificate che presentano il rischio più elevato. Questo controllo ha esito negativo se una qualsiasi delle regole di un gruppo di sicurezza consente il traffico in ingresso da `0.0.0.0/0` o `::/0` verso tali porte. La documentazione relativa a questo controllo consiglia di eliminare le regole che consentono questo traffico.

Oltre ad affrontare la regola del singolo gruppo di sicurezza, questo è un ottimo esempio di scoperta che dovrebbe portare a una nuova AWS Config regola. Utilizzando la modalità di valutazione proattiva, puoi contribuire a prevenire l'implementazione di regole rischiose per i gruppi di sicurezza in futuro. La modalità proattiva valuta le risorse prima che vengano distribuite in modo da evitare configurazioni errate delle risorse e i relativi problemi di sicurezza. Quando implementano un nuovo servizio o una nuova funzionalità, i team applicativi possono eseguire le regole in modalità proattiva nell'ambito della loro pipeline di integrazione e distribuzione continua (CI/CD) per identificare le risorse non conformi. L'immagine seguente mostra come utilizzare una AWS Config regola proattiva per confermare la conformità dell'infrastruttura definita in un modello. AWS CloudFormation



In questo esempio è possibile ottenere un'altra importante efficienza. Quando un team applicativo crea una AWS Config regola proattiva, può condividerla in un archivio di codice comune in modo che altri team applicativi possano utilizzarla.

Ogni risultato associato a un controllo Security Hub contiene dettagli sulla scoperta e un collegamento alle istruzioni per risolvere il problema. Sebbene i team addetti al cloud possano riscontrare risultati che richiedono una correzione manuale e una tantum, se del caso, consigliamo di creare controlli proattivi che identifichino i problemi il prima possibile nel processo di sviluppo.

Segnala e migliora il tuo programma di gestione delle vulnerabilità

Una reportistica efficace per la gestione delle vulnerabilità implica la revisione dei dati, il monitoraggio delle tendenze e la condivisione delle conoscenze. Ciò fornisce visibilità e aiuta i team a migliorare la posizione di sicurezza delle proprie organizzazioni in. Cloud AWS

Conduci riunioni mensili sulle operazioni di sicurezza

Le riunioni mensili sulle operazioni di sicurezza sono un meccanismo efficace per promuovere la titolarità, la responsabilità e l'allineamento continui tra i team. Durante la riunione, le parti interessate dei team addetti alla sicurezza, al cloud e alle applicazioni esaminano i dati alla ricerca di risultati eccezionali in materia di sicurezza, risultati che non rientrano negli accordi sui livelli di servizio (SLA) e individuano i team che hanno ottenuto il maggior numero di risultati.

Queste riunioni aiutano i team a identificare gli schemi contrari, ad esempio le opportunità di aggiungere ulteriori restrizioni. È inoltre possibile scoprire e condividere i controlli preventivi e le opportunità di automazione. Le riunioni aiutano anche a identificare ciò che funziona e ciò che non funziona bene all'interno del programma di gestione delle vulnerabilità, in modo da poter apportare miglioramenti.

Esaminando i dati, identificando modelli e problemi e condividendo informazioni su controlli e automazioni, i team possono ottenere informazioni preziose e apportare continui perfezionamenti in grado di rafforzare il loro livello di sicurezza e ridurre gli SLA relativi alla sicurezza.

Usa le informazioni di Security Hub per identificare gli anti-pattern

AWS Security Hub Gli approfondimenti possono anche aiutarti a identificare gli anti-pattern e a monitorare i progressi compiuti nella correzione dei risultati. Una panoramica di Security Hub è una raccolta di risultati correlati. Identificano un'area di sicurezza che richiede attenzione e intervento. Gli approfondimenti di Security Hub possono aiutarti a identificare requisiti specifici e sviluppare report. Security Hub offre diversi approfondimenti integrati e gestiti. Per tenere traccia dei problemi di sicurezza specifici del tuo AWS ambiente e del tuo utilizzo, puoi creare approfondimenti personalizzati.

Conclusioni e fasi successive

In sintesi, un programma di gestione delle vulnerabilità efficace richiede una preparazione approfondita e richiede l'attivazione degli strumenti e delle integrazioni giusti, la messa a punto di tali strumenti, la valutazione efficiente dei problemi e la creazione di report e miglioramenti continui. Seguendo le best practice riportate in questa guida, le organizzazioni possono creare un programma scalabile di gestione delle vulnerabilità per proteggere i propri ambienti cloud. AWS

È possibile ampliare questo programma per includere ulteriori vulnerabilità e risultati relativi alla sicurezza, come le vulnerabilità di sicurezza delle applicazioni. AWS Security Hub supporta integrazioni di prodotti personalizzate. Prendi in considerazione l'utilizzo di Security Hub come punto di integrazione per strumenti e prodotti di sicurezza aggiuntivi. Questa integrazione ti consente di sfruttare i processi e i flussi di lavoro che hai già stabilito nel tuo programma di gestione delle vulnerabilità, come l'integrazione diretta con i backlog dei prodotti e le riunioni mensili di revisione della sicurezza.

La tabella seguente riassume le fasi e le azioni descritte in questa guida.

Fase	Elementi d'azione
Preparazione	• Definire un piano di gestione delle vulnerabilità. • Distribuisci la proprietà dei risultati. • Sviluppa un programma di divulgazione delle vulnerabilità. • Sviluppa una struttura Account AWS . • Definisci, implementa e applica i tag. • Monitora i AWS bollettini sulla sicurezza. • Abilita Amazon Inspector con un amministratore delegato. • Abilita Security Hub con un amministratore delegato. • Abilita gli standard Security Hub. • Configura l'aggregazione interregionale di Security Hub.

Fase	Elementi d'azione
	• Abilita i risultati del controllo consolidato in Security Hub. • Configura e gestisci le integrazioni del Security Hub, comprese le integrazioni downstream applicabili con SIEM, GRC o sistemi di product backlog o di ticketing
Triage e correzione	• Indirizza i risultati sulla base di una strategia multi-account. • Indirizza i risultati ai team di sicurezza, cloud, applicativi o di sviluppo. • Ottimizza i risultati sulla sicurezza per assicurarti che siano utilizzabili per il tuo ambiente specifico. • Sviluppa meccanismi di riparazione automatizzati, quando possibile. • Implementa controlli della pipeline CI/CD o altri sistemi di protezione che aiutino a prevenire i problemi di sicurezza, quando possibile. • Utilizza le regole di automazione di Security Hub per aumentare o eliminare i risultati.
Segnala e migliora	• Organizza riunioni mensili sulle operazioni di sicurezza. • Usa gli approfondimenti di Security Hub per identificare gli anti-pattern.

Risorse

AWS documentazione di servizio

- Integrazioni di prodotti ()AWS Security Hub
- Integrazione AWS Security Hub in Jira Service Management Cloud ()AWS Security Hub
- Regole di automazione ()AWS Security Hub
- Regole di valutazione proattiva ()AWS Config
- Patch Manager ()AWS Systems Manager

Altre AWS risorse

- Migliori pratiche per etichettare AWS le risorse (AWS white paper)
- Risposta di sicurezza automatizzata su AWS (Solutions Library)AWS
- AWS Guida alla risposta agli incidenti di sicurezza (guida AWS tecnica)
- AWS bollettini sulla sicurezza

Cronologia dei documenti

La tabella seguente descrive le modifiche significative apportate a questa guida. Per ricevere notifiche sugli aggiornamenti futuri, puoi abbonarti a un feed RSS.

Modifica	Descrizione	Data
Pubblicazione iniziale	—	12 ottobre 2023

AWS Glossario delle linee guida prescrittive

I seguenti sono termini comunemente usati nelle strategie, nelle guide e nei modelli forniti da AWS Prescriptive Guidance. Per suggerire voci, utilizza il link Fornisci feedback alla fine del glossario.

Numeri

7 R

Sette strategie di migrazione comuni per trasferire le applicazioni sul cloud. Queste strategie si basano sulle 5 R identificate da Gartner nel 2011 e sono le seguenti:

- Rifattorizzare/riprogettare: trasferisci un'applicazione e modifica la sua architettura sfruttando appieno le funzionalità native del cloud per migliorare l'agilità, le prestazioni e la scalabilità. Ciò comporta in genere la portabilità del sistema operativo e del database. Esempio: migra il tuo database Oracle locale all'edizione compatibile con Amazon Aurora PostgreSQL.
- Ridefinire la piattaforma (lift and reshape): trasferisci un'applicazione nel cloud e introduci un certo livello di ottimizzazione per sfruttare le funzionalità del cloud. Esempio: migra il tuo database Oracle locale ad Amazon Relational Database Service (Amazon RDS) per Oracle in. Cloud AWS
- Riacquistare (drop and shop): passa a un prodotto diverso, in genere effettuando la transizione da una licenza tradizionale a un modello SaaS. Esempio: migra il tuo sistema di gestione delle relazioni con i clienti (CRM) su Salesforce.com.
- Eseguire il rehosting (lift and shift): trasferisci un'applicazione sul cloud senza apportare modifiche per sfruttare le funzionalità del cloud. Esempio: migra il tuo database Oracle locale a Oracle su un'istanza EC2 in. Cloud AWS
- Trasferire (eseguire il rehosting a livello hypervisor): trasferisci l'infrastruttura sul cloud senza acquistare nuovo hardware, riscrivere le applicazioni o modificare le operazioni esistenti. Esegui la migrazione dei server da una piattaforma locale a un servizio cloud per la stessa piattaforma. Esempio: migra un'applicazione suMicrosoft Hyper-V. AWS
- Riesaminare (mantenere): mantieni le applicazioni nell'ambiente di origine. Queste potrebbero includere applicazioni che richiedono una rifattorizzazione significativa che desideri rimandare a un momento successivo e applicazioni legacy che desideri mantenere, perché non vi è alcuna giustificazione aziendale per effettuarne la migrazione.
- Ritirare: disattiva o rimuovi le applicazioni che non sono più necessarie nell'ambiente di origine.

A

ABAC

Vedi controllo degli accessi basato sugli attributi.

servizi astratti

Vedi servizi gestiti.

ACIDO

Vedi atomicità, consistenza, isolamento, durata.

migrazione attiva-attiva

Un metodo di migrazione del database in cui i database di origine e di destinazione vengono mantenuti sincronizzati (utilizzando uno strumento di replica bidirezionale o operazioni di doppia scrittura) ed entrambi i database gestiscono le transazioni provenienti dalle applicazioni di connessione durante la migrazione. Questo metodo supporta la migrazione in piccoli batch controllati anziché richiedere una conversione una tantum. È più flessibile ma richiede più lavoro rispetto alla migrazione attiva-passiva.

migrazione attiva-passiva

Un metodo di migrazione di database in cui i database di origine e di destinazione vengono mantenuti sincronizzati, ma solo il database di origine gestisce le transazioni provenienti dalle applicazioni di connessione mentre i dati vengono replicati nel database di destinazione. Il database di destinazione non accetta alcuna transazione durante la migrazione.

funzione aggregata

Una funzione SQL che opera su un gruppo di righe e calcola un singolo valore restituito per il gruppo. Esempi di funzioni aggregate includono `SUM` e. `MAX`

Intelligenza artificiale

Vedi intelligenza artificiale.

AIOps

Guarda le operazioni di intelligenza artificiale.

anonimizzazione

Il processo di eliminazione permanente delle informazioni personali in un set di dati. L'anonimizzazione può aiutare a proteggere la privacy personale. I dati anonimi non sono più considerati dati personali.

anti-modello

Una soluzione utilizzata frequentemente per un problema ricorrente in cui la soluzione è controproducente, inefficace o meno efficace di un'alternativa.

controllo delle applicazioni

Un approccio alla sicurezza che consente l'uso solo di applicazioni approvate per proteggere un sistema dal malware.

portfolio di applicazioni

Una raccolta di informazioni dettagliate su ogni applicazione utilizzata da un'organizzazione, compresi i costi di creazione e manutenzione dell'applicazione e il relativo valore aziendale. Queste informazioni sono fondamentali per il processo di scoperta e analisi del portfolio e aiutano a identificare e ad assegnare la priorità alle applicazioni da migrare, modernizzare e ottimizzare.

intelligenza artificiale (IA)

Il campo dell'informatica dedicato all'uso delle tecnologie informatiche per svolgere funzioni cognitive tipicamente associate agli esseri umani, come l'apprendimento, la risoluzione di problemi e il riconoscimento di schemi. Per ulteriori informazioni, consulta la sezione Che cos'è l'intelligenza artificiale?

operazioni di intelligenza artificiale (AIOps)

Il processo di utilizzo delle tecniche di machine learning per risolvere problemi operativi, ridurre gli incidenti operativi e l'intervento umano e aumentare la qualità del servizio. Per ulteriori informazioni su come viene utilizzato AIOps nella strategia di migrazione AWS , consulta la guida all'integrazione delle operazioni.

crittografia asimmetrica

Un algoritmo di crittografia che utilizza una coppia di chiavi, una chiave pubblica per la crittografia e una chiave privata per la decrittografia. Puoi condividere la chiave pubblica perché non viene utilizzata per la decrittografia, ma l'accesso alla chiave privata deve essere altamente limitato.

atomicità, consistenza, isolamento, durabilità (ACID)

Un insieme di proprietà del software che garantiscono la validità dei dati e l'affidabilità operativa di un database, anche in caso di errori, interruzioni di corrente o altri problemi.

Controllo degli accessi basato su attributi (ABAC)

La pratica di creare autorizzazioni dettagliate basate su attributi utente, come reparto, ruolo professionale e nome del team. Per ulteriori informazioni, consulta ABAC for AWS nella documentazione AWS Identity and Access Management (IAM).

fonte di dati autorevole

Una posizione in cui è archiviata la versione principale dei dati, considerata la fonte di informazioni più affidabile. È possibile copiare i dati dalla fonte di dati autorevole in altre posizioni allo scopo di elaborarli o modificarli, ad esempio anonimizzandoli, oscurandoli o pseudonimizzandoli.

Zona di disponibilità

Una posizione distinta all'interno di un edificio Regione AWS che è isolata dai guasti in altre zone di disponibilità e offre una connettività di rete economica e a bassa latenza verso altre zone di disponibilità nella stessa regione.

AWS Cloud Adoption Framework (CAF)AWS

Un framework di linee guida e best practice AWS per aiutare le organizzazioni a sviluppare un piano efficiente ed efficace per passare con successo al cloud. AWS CAF organizza le linee guida in sei aree di interesse chiamate prospettive: business, persone, governance, piattaforma, sicurezza e operazioni. Le prospettive relative ad azienda, persone e governance si concentrano sulle competenze e sui processi aziendali; le prospettive relative alla piattaforma, alla sicurezza e alle operazioni si concentrano sulle competenze e sui processi tecnici. Ad esempio, la prospettiva relativa alle persone si rivolge alle parti interessate che gestiscono le risorse umane (HR), le funzioni del personale e la gestione del personale. In questa prospettiva, AWS CAF fornisce linee guida per lo sviluppo delle persone, la formazione e le comunicazioni per aiutare a preparare l'organizzazione all'adozione del cloud di successo. Per ulteriori informazioni, consulta il sito web di AWS CAF e il white paper AWS CAF.

AWS Workload Qualification Framework (WQF)AWS

Uno strumento che valuta i carichi di lavoro di migrazione dei database, consiglia strategie di migrazione e fornisce stime del lavoro. AWS WQF è incluso in (). AWS Schema Conversion Tool AWS SCT Analizza gli schemi di database e gli oggetti di codice, il codice dell'applicazione, le dipendenze e le caratteristiche delle prestazioni e fornisce report di valutazione.

B

bot difettoso

Un bot che ha lo scopo di disturbare o causare danni a individui o organizzazioni.

BCP

Vedi la pianificazione della continuità operativa.

grafico comportamentale

Una vista unificata, interattiva dei comportamenti delle risorse e delle interazioni nel tempo. Puoi utilizzare un grafico comportamentale con Amazon Detective per esaminare tentativi di accesso non riusciti, chiamate API sospette e azioni simili. Per ulteriori informazioni, consulta Dati in un grafico comportamentale nella documentazione di Detective.

sistema big-endian

Un sistema che memorizza per primo il byte più importante. Vedi anche endianness.

Classificazione binaria

Un processo che prevede un risultato binario (una delle due classi possibili). Ad esempio, il modello di machine learning potrebbe dover prevedere problemi come "Questa e-mail è spam o non è spam?" o "Questo prodotto è un libro o un'auto?"

filtro Bloom

Una struttura di dati probabilistica ed efficiente in termini di memoria che viene utilizzata per verificare se un elemento fa parte di un set.

distribuzioni blu/verdi

Una strategia di implementazione in cui si creano due ambienti separati ma identici. La versione corrente dell'applicazione viene eseguita in un ambiente (blu) e la nuova versione dell'applicazione nell'altro ambiente (verde). Questa strategia consente di ripristinare rapidamente il sistema con un impatto minimo.

bot

Un'applicazione software che esegue attività automatizzate su Internet e simula l'attività o l'interazione umana. Alcuni bot sono utili o utili, come i web crawler che indicizzano le informazioni su Internet. Alcuni altri bot, noti come bot dannosi, hanno lo scopo di disturbare o causare danni a individui o organizzazioni.

botnet

Reti di bot infettate da malware e controllate da un'unica parte, nota come bot herder o bot operator. Le botnet sono il meccanismo più noto per scalare i bot e il loro impatto.

ramo

Un'area contenuta di un repository di codice. Il primo ramo creato in un repository è il ramo principale. È possibile creare un nuovo ramo a partire da un ramo esistente e quindi sviluppare funzionalità o correggere bug al suo interno. Un ramo creato per sviluppare una funzionalità viene comunemente detto ramo di funzionalità. Quando la funzionalità è pronta per il rilascio, il ramo di funzionalità viene ricongiunto al ramo principale. Per ulteriori informazioni, consulta Informazioni sulle filiali (documentazione). GitHub

accesso break-glass

In circostanze eccezionali e tramite una procedura approvata, un mezzo rapido per consentire a un utente di accedere a un sito a Account AWS cui in genere non dispone delle autorizzazioni necessarie. Per ulteriori informazioni, vedere l'indicatore Implementate break-glass procedures nella guida Well-Architected AWS .

strategia brownfield

L'infrastruttura esistente nell'ambiente. Quando si adotta una strategia brownfield per un'architettura di sistema, si progetta l'architettura in base ai vincoli dei sistemi e dell'infrastruttura attuali. Per l'espansione dell'infrastruttura esistente, è possibile combinare strategie brownfield e greenfield.

cache del buffer

L'area di memoria in cui sono archiviati i dati a cui si accede con maggiore frequenza.

capacità di business

Azioni intraprese da un'azienda per generare valore (ad esempio vendite, assistenza clienti o marketing). Le architetture dei microservizi e le decisioni di sviluppo possono essere guidate dalle capacità aziendali. Per ulteriori informazioni, consulta la sezione Organizzazione in base alle funzionalità aziendali del whitepaper Esecuzione di microservizi containerizzati su AWS.

pianificazione della continuità operativa (BCP)

Un piano che affronta il potenziale impatto di un evento che comporta l'interruzione dell'attività, come una migrazione su larga scala, sulle operazioni e consente a un'azienda di riprendere rapidamente le operazioni.

C

CAF

Vedi AWS Cloud Adoption Framework.

implementazione canaria

Il rilascio lento e incrementale di una versione agli utenti finali. Quando sei sicuro, distribuisci la nuova versione e sostituisci la versione corrente nella sua interezza.

CoE

Vedi Cloud Center of Excellence.

CDC

Vedi Change Data Capture.

Change Data Capture (CDC)

Il processo di tracciamento delle modifiche a un'origine dati, ad esempio una tabella di database, e di registrazione dei metadati relativi alla modifica. È possibile utilizzare CDC per vari scopi, ad esempio il controllo o la replica delle modifiche in un sistema di destinazione per mantenere la sincronizzazione.

ingegneria del caos

Introduzione intenzionale di guasti o eventi dirompenti per testare la resilienza di un sistema. Puoi usare AWS Fault Injection Service (AWS FIS) per eseguire esperimenti che stressano i tuoi AWS carichi di lavoro e valutarne la risposta.

CI/CD

Vedi integrazione continua e distribuzione continua.

classificazione

Un processo di categorizzazione che aiuta a generare previsioni. I modelli di ML per problemi di classificazione prevedono un valore discreto. I valori discreti sono sempre distinti l'uno dall'altro. Ad esempio, un modello potrebbe dover valutare se in un'immagine è presente o meno un'auto.

crittografia lato client

Crittografia dei dati a livello locale, prima che il destinatario li AWS servizio riceva.

centro di eccellenza del cloud (CCoE)

Un team multidisciplinare che guida le iniziative di adozione del cloud in tutta l'organizzazione, tra cui lo sviluppo di best practice per il cloud, la mobilitazione delle risorse, la definizione delle tempistiche di migrazione e la guida dell'organizzazione attraverso trasformazioni su larga scala. Per ulteriori informazioni, consulta i post di CCoE sull' Cloud AWS Enterprise Strategy Blog.

cloud computing

La tecnologia cloud generalmente utilizzata per l'archiviazione remota di dati e la gestione dei dispositivi IoT. Il cloud computing è generalmente collegato alla tecnologia di edge computing.

modello operativo cloud

In un'organizzazione IT, il modello operativo utilizzato per creare, maturare e ottimizzare uno o più ambienti cloud. Per ulteriori informazioni, consulta Building your Cloud Operating Model.

fasi di adozione del cloud

Le quattro fasi che le organizzazioni in genere attraversano quando migrano verso Cloud AWS:

- Progetto: esecuzione di alcuni progetti relativi al cloud per scopi di dimostrazione e apprendimento
- Fondamento: effettuare investimenti fondamentali per dimensionare l'adozione del cloud (ad esempio, creazione di una zona di destinazione, definizione di un CCoE, definizione di un modello operativo)
- Migrazione: migrazione di singole applicazioni
- Reinvenzione: ottimizzazione di prodotti e servizi e innovazione nel cloud

Queste fasi sono state definite da Stephen Orban nel post del blog The Journey Toward Cloud-First & the Stages of Adoption on the Enterprise Strategy. Cloud AWS Per informazioni su come si relazionano alla strategia di AWS migrazione, consulta la guida alla preparazione alla migrazione.

CMDB

Vedi database di gestione della configurazione.

repository di codice

Una posizione in cui il codice di origine e altri asset, come documentazione, esempi e script, vengono archiviati e aggiornati attraverso processi di controllo delle versioni. Gli archivi cloud più comuni includono GitHub o AWS CodeCommit. Ogni versione del codice è denominata ramo. In

una struttura a microservizi, ogni repository è dedicato a una singola funzionalità. Una singola pipeline CI/CD può utilizzare più repository.

cache fredda

Una cache del buffer vuota, non ben popolata o contenente dati obsoleti o irrilevanti. Ciò influisce sulle prestazioni perché l'istanza di database deve leggere dalla memoria o dal disco principale, il che richiede più tempo rispetto alla lettura dalla cache del buffer.

dati freddi

Dati a cui si accede raramente e che in genere sono storici. Quando si eseguono interrogazioni di questo tipo di dati, le interrogazioni lente sono in genere accettabili. Lo spostamento di questi dati su livelli o classi di storage meno costosi e con prestazioni inferiori può ridurre i costi.

visione artificiale (CV)

Un campo dell'intelligenza artificiale che utilizza l'apprendimento automatico per analizzare ed estrarre informazioni da formati visivi come immagini e video digitali. Ad esempio, AWS Panorama offre dispositivi che aggiungono CV alle reti di telecamere locali e Amazon SageMaker fornisce algoritmi di elaborazione delle immagini per CV.

deriva della configurazione

Per un carico di lavoro, una modifica della configurazione rispetto allo stato previsto. Potrebbe causare la non conformità del carico di lavoro e in genere è graduale e involontaria.

database di gestione della configurazione (CMDB)

Un repository che archivia e gestisce le informazioni su un database e il relativo ambiente IT, inclusi i componenti hardware e software e le relative configurazioni. In genere si utilizzano i dati di un CMDB nella fase di individuazione e analisi del portafoglio della migrazione.

Pacchetto di conformità

Una raccolta di AWS Config regole e azioni correttive che puoi assemblare per personalizzare i controlli di conformità e sicurezza. È possibile distribuire un pacchetto di conformità come singola entità in una regione Account AWS and o all'interno di un'organizzazione utilizzando un modello YAML. Per ulteriori informazioni, consulta i Conformance Pack nella documentazione. AWS Config

integrazione e distribuzione continua (continuous integration and continuous delivery, CI/CD)

Il processo di automazione delle fasi di origine, creazione, test, gestione temporanea e produzione del processo di rilascio del software. Il processo CI/CD è comunemente descritto come una

pipeline. CI/CD può aiutare ad automatizzare i processi, migliorare la produttività, migliorare la qualità del codice e velocizzare le distribuzioni. Per ulteriori informazioni, consulta Vantaggi della distribuzione continua. CD può anche significare continuous deployment (implementazione continua). Per ulteriori informazioni, consulta Distribuzione continua e implementazione continua a confronto.

CV

Vedi visione artificiale.

D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

Un processo per identificare e classificare i dati nella rete in base alla loro criticità e sensibilità. È un componente fondamentale di qualsiasi strategia di gestione dei rischi di sicurezza informatica perché consente di determinare i controlli di protezione e conservazione appropriati per i dati. La classificazione dei dati è un componente del pilastro della sicurezza nel AWS Well-Architected Framework. Per ulteriori informazioni, consulta Classificazione dei dati.

deriva dei dati

Una variazione significativa tra i dati di produzione e i dati utilizzati per addestrare un modello di machine learning o una modifica significativa dei dati di input nel tempo. La deriva dei dati può ridurre la qualità, l'accuratezza e l'equità complessive nelle previsioni dei modelli ML.

dati in transito

Dati che si spostano attivamente attraverso la rete, ad esempio tra le risorse di rete.

rete di dati

Un framework architettonico che fornisce la proprietà distribuita e decentralizzata dei dati con gestione e governance centralizzate.

riduzione al minimo dei dati

Il principio della raccolta e del trattamento dei soli dati strettamente necessari. Praticare la riduzione al minimo dei dati in the Cloud AWS può ridurre i rischi per la privacy, i costi e l'impronta di carbonio delle analisi.

perimetro dei dati

Una serie di barriere preventive nell' AWS ambiente che aiutano a garantire che solo le identità attendibili accedano alle risorse attendibili delle reti previste. Per ulteriori informazioni, consulta Building a data perimeter on. AWS

pre-elaborazione dei dati

Trasformare i dati grezzi in un formato che possa essere facilmente analizzato dal modello di ML. La pre-elaborazione dei dati può comportare la rimozione di determinate colonne o righe e l'eliminazione di valori mancanti, incoerenti o duplicati.

provenienza dei dati

Il processo di tracciamento dell'origine e della cronologia dei dati durante il loro ciclo di vita, ad esempio il modo in cui i dati sono stati generati, trasmessi e archiviati.

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

Un sistema di gestione dei dati che supporta la business intelligence, come l'analisi. I data warehouse contengono in genere grandi quantità di dati storici e vengono generalmente utilizzati per interrogazioni e analisi.

linguaggio di definizione del database (DDL)

Istruzioni o comandi per creare o modificare la struttura di tabelle e oggetti in un database.

linguaggio di manipolazione del database (DML)

Istruzioni o comandi per modificare (inserire, aggiornare ed eliminare) informazioni in un database.

DDL

Vedi linguaggio di definizione del database.

deep ensemble

Combinare più modelli di deep learning per la previsione. È possibile utilizzare i deep ensemble per ottenere una previsione più accurata o per stimare l'incertezza nelle previsioni.

deep learning

Un sottocampo del ML che utilizza più livelli di reti neurali artificiali per identificare la mappatura tra i dati di input e le variabili target di interesse.

defense-in-depth

Un approccio alla sicurezza delle informazioni in cui una serie di meccanismi e controlli di sicurezza sono accuratamente stratificati su una rete di computer per proteggere la riservatezza, l'integrità e la disponibilità della rete e dei dati al suo interno. Quando si adotta questa strategia AWS, si aggiungono più controlli a diversi livelli della AWS Organizations struttura per proteggere le risorse. Ad esempio, un defense-in-depth approccio potrebbe combinare l'autenticazione a più fattori, la segmentazione della rete e la crittografia.

amministratore delegato

In AWS Organizations, un servizio compatibile può registrare un account AWS membro per amministrare gli account dell'organizzazione e gestire le autorizzazioni per quel servizio. Questo account è denominato amministratore delegato per quel servizio specifico. Per ulteriori informazioni e un elenco di servizi compatibili, consulta Servizi che funzionano con AWS Organizations nella documentazione di AWS Organizations .

implementazione

Il processo di creazione di un'applicazione, di nuove funzionalità o di correzioni di codice disponibili nell'ambiente di destinazione. L'implementazione prevede l'applicazione di modifiche in una base di codice, seguita dalla creazione e dall'esecuzione di tale base di codice negli ambienti applicativi.

Ambiente di sviluppo

Vedi ambiente.

controllo di rilevamento

Un controllo di sicurezza progettato per rilevare, registrare e avvisare dopo che si è verificato un evento. Questi controlli rappresentano una seconda linea di difesa e avvisano l'utente in caso di eventi di sicurezza che aggirano i controlli preventivi in vigore. Per ulteriori informazioni, consulta Controlli di rilevamento in Implementazione dei controlli di sicurezza in AWS.

mappatura del flusso di valore dello sviluppo (DVSM)

Un processo utilizzato per identificare e dare priorità ai vincoli che influiscono negativamente sulla velocità e sulla qualità nel ciclo di vita dello sviluppo del software. DVSM estende il processo di

mappatura del flusso di valore originariamente progettato per pratiche di produzione snella. Si concentra sulle fasi e sui team necessari per creare e trasferire valore attraverso il processo di sviluppo del software.

gemello digitale

Una rappresentazione virtuale di un sistema reale, ad esempio un edificio, una fabbrica, un'attrezzatura industriale o una linea di produzione. I gemelli digitali supportano la manutenzione predittiva, il monitoraggio remoto e l'ottimizzazione della produzione.

tabella delle dimensioni

In uno schema a stella, una tabella più piccola che contiene gli attributi dei dati quantitativi in una tabella dei fatti. Gli attributi della tabella delle dimensioni sono in genere campi di testo o numeri discreti che si comportano come testo. Questi attributi vengono comunemente utilizzati per il vincolo delle query, il filtraggio e l'etichettatura dei set di risultati.

disastro

Un evento che impedisce a un carico di lavoro o a un sistema di raggiungere gli obiettivi aziendali nella sua sede principale di implementazione. Questi eventi possono essere disastri naturali, guasti tecnici o il risultato di azioni umane, come errori di configurazione involontari o attacchi di malware.

disaster recovery (DR)

La strategia e il processo utilizzati per ridurre al minimo i tempi di inattività e la perdita di dati causati da un disastro. Per ulteriori informazioni, consulta Disaster Recovery of Workloads su AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

Un approccio allo sviluppo di un sistema software complesso collegandone i componenti a domini in evoluzione, o obiettivi aziendali principali, perseguiti da ciascun componente. Questo concetto è stato introdotto da Eric Evans nel suo libro,Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003). Per informazioni su come utilizzare la progettazione basata sul dominio con il modello del fico strangolatore (Strangler Fig), consulta la sezione Modernizzazione incrementale dei servizi Web Microsoft ASP.NET (ASMX) legacy utilizzando container e il Gateway Amazon API.

DOTT.

Vedi disaster recovery.

rilevamento della deriva

Tracciamento delle deviazioni da una configurazione di base. Ad esempio, è possibile AWS CloudFormation utilizzarlo per rilevare deviazioni nelle risorse di sistema oppure AWS Control Tower per rilevare cambiamenti nella landing zone che potrebbero influire sulla conformità ai requisiti di governance.

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

E

EDA

Vedi analisi esplorativa dei dati.

edge computing

La tecnologia che aumenta la potenza di calcolo per i dispositivi intelligenti all'edge di una rete IoT. Rispetto al cloud computing, l'edge computing può ridurre la latenza di comunicazione e migliorare i tempi di risposta.

crittografia

Un processo di elaborazione che trasforma i dati in chiaro, leggibili dall'uomo, in testo cifrato.

chiave crittografica

Una stringa crittografica di bit randomizzati generata da un algoritmo di crittografia. Le chiavi possono variare di lunghezza e ogni chiave è progettata per essere imprevedibile e univoca.

endianità

L'ordine in cui i byte vengono archiviati nella memoria del computer. I sistemi big-endian memorizzano per primo il byte più importante. I sistemi little-endian memorizzano per primo il byte meno importante.

endpoint

Vedi service endpoint.

servizio endpoint

Un servizio che puoi ospitare in un cloud privato virtuale (VPC) da condividere con altri utenti. Puoi creare un servizio endpoint con AWS PrivateLink e concedere autorizzazioni ad altri Account AWS o a AWS Identity and Access Management (IAM) principali. Questi account o principali possono connettersi al servizio endpoint in privato creando endpoint VPC di interfaccia. Per ulteriori informazioni, consulta Creazione di un servizio endpoint nella documentazione di Amazon Virtual Private Cloud (Amazon VPC).

pianificazione delle risorse aziendali (ERP)

Un sistema che automatizza e gestisce i processi aziendali chiave (come contabilità, MES e gestione dei progetti) per un'azienda.

crittografia envelope

Il processo di crittografia di una chiave di crittografia con un'altra chiave di crittografia. Per ulteriori informazioni, vedete Envelope encryption nella documentazione AWS Key Management Service (AWS KMS).

ambiente

Un'istanza di un'applicazione in esecuzione. Di seguito sono riportati i tipi di ambiente più comuni nel cloud computing:

- ambiente di sviluppo: un'istanza di un'applicazione in esecuzione disponibile solo per il team principale responsabile della manutenzione dell'applicazione. Gli ambienti di sviluppo vengono utilizzati per testare le modifiche prima di promuoverle negli ambienti superiori. Questo tipo di ambiente viene talvolta definito ambiente di test.
- ambienti inferiori: tutti gli ambienti di sviluppo di un'applicazione, ad esempio quelli utilizzati per le build e i test iniziali.
- ambiente di produzione: un'istanza di un'applicazione in esecuzione a cui gli utenti finali possono accedere. In una pipeline CI/CD, l'ambiente di produzione è l'ultimo ambiente di implementazione.
- ambienti superiori: tutti gli ambienti a cui possono accedere utenti diversi dal team di sviluppo principale. Si può trattare di un ambiente di produzione, ambienti di preproduzione e ambienti per i test di accettazione da parte degli utenti.

epica

Nelle metodologie agili, categorie funzionali che aiutano a organizzare e dare priorità al lavoro. Le epiche forniscono una descrizione di alto livello dei requisiti e delle attività di implementazione.

Ad esempio, le epopee della sicurezza AWS CAF includono la gestione delle identità e degli accessi, i controlli investigativi, la sicurezza dell'infrastruttura, la protezione dei dati e la risposta agli incidenti. Per ulteriori informazioni sulle epiche, consulta la strategia di migrazione AWS , consulta la guida all'implementazione del programma.

ERP

Vedi la pianificazione delle risorse aziendali.

analisi esplorativa dei dati (EDA)

Il processo di analisi di un set di dati per comprenderne le caratteristiche principali. Si raccolgono o si aggregano dati e quindi si eseguono indagini iniziali per trovare modelli, rilevare anomalie e verificare ipotesi. L'EDA viene eseguita calcolando statistiche di riepilogo e creando visualizzazioni di dati.

F

tabella dei fatti

Il tavolo centrale in uno schema a stella. Memorizza dati quantitativi sulle operazioni aziendali. In genere, una tabella dei fatti contiene due tipi di colonne: quelle che contengono misure e quelle che contengono una chiave esterna per una tabella di dimensioni.

fallire velocemente

Una filosofia che utilizza test frequenti e incrementali per ridurre il ciclo di vita dello sviluppo. È una parte fondamentale di un approccio agile.

limite di isolamento dei guasti

Nel Cloud AWS, un limite come una zona di disponibilità Regione AWS, un piano di controllo o un piano dati che limita l'effetto di un errore e aiuta a migliorare la resilienza dei carichi di lavoro. Per ulteriori informazioni, consulta AWS Fault Isolation Boundaries.

ramo di funzionalità

Vedi filiale.

caratteristiche

I dati di input che usi per fare una previsione. Ad esempio, in un contesto di produzione, le caratteristiche potrebbero essere immagini acquisite periodicamente dalla linea di produzione.

importanza delle caratteristiche

Quanto è importante una caratteristica per le previsioni di un modello. Di solito viene espresso come punteggio numerico che può essere calcolato con varie tecniche, come Shapley Additive Explanations (SHAP) e gradienti integrati. Per ulteriori informazioni, vedere Interpretabilità del modello di machine learning con:AWS.

trasformazione delle funzionalità

Per ottimizzare i dati per il processo di machine learning, incluso l'arricchimento dei dati con fonti aggiuntive, il dimensionamento dei valori o l'estrazione di più set di informazioni da un singolo campo di dati. Ciò consente al modello di ML di trarre vantaggio dai dati. Ad esempio, se suddividi la data "2021-05-27 00:15:37" in "2021", "maggio", "giovedì" e "15", puoi aiutare l'algoritmo di apprendimento ad apprendere modelli sfumati associati a diversi componenti dei dati.

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

L'uso di più condizioni per consentire o rifiutare una richiesta di accesso.

migrazione flash-cut

Un metodo di migrazione del database che utilizza la replica continua dei dati tramite l'acquisizione dei dati delle modifiche per migrare i dati nel più breve tempo possibile, anziché utilizzare un approccio graduale. L'obiettivo è ridurre al minimo i tempi di inattività.

G

blocco geografico

Vedi restrizioni geografiche.

limitazioni geografiche (blocco geografico)

In Amazon CloudFront, un'opzione per impedire agli utenti di determinati paesi di accedere alle distribuzioni di contenuti. Puoi utilizzare un elenco consentito o un elenco di blocco per specificare i paesi approvati e vietati. Per ulteriori informazioni, consulta Limitare la distribuzione geografica dei contenuti nella CloudFront documentazione.

Flusso di lavoro di GitFlow

Un approccio in cui gli ambienti inferiori e superiori utilizzano rami diversi in un repository di codice di origine. Il flusso di lavoro Gitflow è considerato obsoleto e il flusso di lavoro basato su trunk è l'approccio moderno e preferito.

strategia greenfield

L'assenza di infrastrutture esistenti in un nuovo ambiente. Quando si adotta una strategia greenfield per un'architettura di sistema, è possibile selezionare tutte le nuove tecnologie senza il vincolo della compatibilità con l'infrastruttura esistente, nota anche come brownfield. Per l'espansione dell'infrastruttura esistente, è possibile combinare strategie brownfield e greenfield.

guardrail

Una regola di livello elevato che consente di governare risorse, policy e conformità tra le unità organizzative (OU). I guardrail preventivi applicano le policy per garantire l'allineamento agli standard di conformità. Vengono implementati utilizzando le policy di controllo dei servizi e i limiti delle autorizzazioni IAM. I guardrail di rilevamento rilevano le violazioni delle policy e i problemi di conformità e generano avvisi per porvi rimedio. Sono implementati utilizzando Amazon AWS Config AWS Security Hub GuardDuty AWS Trusted Advisor, Amazon Inspector e controlli personalizzati AWS Lambda .

H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

Migrazione del database di origine in un database di destinazione che utilizza un motore di database diverso (ad esempio, da Oracle ad Amazon Aurora). La migrazione eterogenea fa in genere parte di uno sforzo di riprogettazione e la conversione dello schema può essere un'attività complessa. AWS offre AWS SCT che aiuta con le conversioni dello schema.

alta disponibilità (HA)

La capacità di un carico di lavoro di funzionare in modo continuo, senza intervento, in caso di sfide o disastri. I sistemi HA sono progettati per il failover automatico, fornire costantemente prestazioni di alta qualità e gestire carichi e guasti diversi con un impatto minimo sulle prestazioni.

modernizzazione storica

Un approccio utilizzato per modernizzare e aggiornare i sistemi di tecnologia operativa (OT) per soddisfare meglio le esigenze dell'industria manifatturiera. Uno storico è un tipo di database utilizzato per raccogliere e archiviare dati da varie fonti in una fabbrica.

migrazione di database omogenea

Migrazione del database di origine in un database di destinazione che condivide lo stesso motore di database (ad esempio, da Microsoft SQL Server ad Amazon RDS per SQL Server). La migrazione omogenea fa in genere parte di un'operazione di rehosting o ridefinizione della piattaforma. Per migrare lo schema è possibile utilizzare le utilità native del database.

dati caldi

Dati a cui si accede frequentemente, ad esempio dati in tempo reale o dati di traduzione recenti. Questi dati richiedono in genere un livello o una classe di storage ad alte prestazioni per fornire risposte rapide alle query.

hotfix

Una soluzione urgente per un problema critico in un ambiente di produzione. A causa della sua urgenza, un hotfix viene in genere creato al di fuori del tipico DevOps flusso di lavoro di rilascio.

periodo di hypercare

Subito dopo la conversione, il periodo di tempo in cui un team di migrazione gestisce e monitora le applicazioni migrate nel cloud per risolvere eventuali problemi. In genere, questo periodo dura da 1 a 4 giorni. Al termine del periodo di hypercare, il team addetto alla migrazione in genere trasferisce la responsabilità delle applicazioni al team addetto alle operazioni cloud.

I

IaC

Considera l'infrastruttura come codice.

Policy basata su identità

Una policy associata a uno o più principi IAM che definisce le relative autorizzazioni all'interno dell' Cloud AWS ambiente.

applicazione inattiva

Un'applicazione che prevede un uso di CPU e memoria medio compreso tra il 5% e il 20% in un periodo di 90 giorni. In un progetto di migrazione, è normale ritirare queste applicazioni o mantenerle on-premise.

IIoT

Vedi Industrial Internet of Things.

infrastruttura immutabile

Un modello che implementa una nuova infrastruttura per i carichi di lavoro di produzione anziché aggiornare, applicare patch o modificare l'infrastruttura esistente. Le infrastrutture immutabili sono intrinsecamente più coerenti, affidabili e prevedibili delle infrastrutture mutabili. Per ulteriori informazioni, consulta la best practice Deploy using immutable infrastructure in Well-Architected AWS Framework.

VPC in ingresso (ingress)

In un'architettura AWS multi-account, un VPC che accetta, ispeziona e indirizza le connessioni di rete dall'esterno di un'applicazione. Nel documento Architettura di riferimento per la sicurezza di AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

migrazione incrementale

Una strategia di conversione in cui si esegue la migrazione dell'applicazione in piccole parti anziché eseguire una conversione singola e completa. Ad esempio, inizialmente potresti spostare solo alcuni microservizi o utenti nel nuovo sistema. Dopo aver verificato che tutto funzioni correttamente, puoi spostare in modo incrementale microservizi o utenti aggiuntivi fino alla disattivazione del sistema legacy. Questa strategia riduce i rischi associati alle migrazioni di grandi dimensioni.

Industria 4.0

Un termine introdotto da Klaus Schwab nel 2016 per riferirsi alla modernizzazione dei processi di produzione attraverso progressi in termini di connettività, dati in tempo reale, automazione, analisi e AI/ML.

infrastruttura

Tutte le risorse e gli asset contenuti nell'ambiente di un'applicazione.

infrastruttura come codice (IaC)

Il processo di provisioning e gestione dell'infrastruttura di un'applicazione tramite un insieme di file di configurazione. Il processo IaC è progettato per aiutarti a centralizzare la gestione dell'infrastruttura, a standardizzare le risorse e a dimensionare rapidamente, in modo che i nuovi ambienti siano ripetibili, affidabili e coerenti.

Internet delle cose industriale (IIoT)

L'uso di sensori e dispositivi connessi a Internet nei settori industriali, come quello manifatturiero, energetico, automobilistico, sanitario, delle scienze della vita e dell'agricoltura. Per ulteriori informazioni, consulta Creazione di una strategia di trasformazione digitale dell'Internet delle cose industriale (IIoT).

VPC di ispezione

In un'architettura AWS multi-account, un VPC centralizzato che gestisce le ispezioni del traffico di rete tra VPC (uguali o diversi Regioni AWS), Internet e reti locali. Nel documento Architettura di riferimento per la sicurezza di AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

Internet of Things (IoT)

La rete di oggetti fisici connessi con sensori o processori incorporati che comunicano con altri dispositivi e sistemi tramite Internet o una rete di comunicazione locale. Per ulteriori informazioni, consulta Cos'è l'IoT?

interpretabilità

Una caratteristica di un modello di machine learning che descrive il grado in cui un essere umano è in grado di comprendere in che modo le previsioni del modello dipendono dai suoi input. Per ulteriori informazioni, consulta la sezione Interpretabilità dei modelli di machine learning con AWS.

IoT

Vedi Internet of Things.

libreria di informazioni IT (ITIL)

Una serie di best practice per offrire servizi IT e allinearli ai requisiti aziendali. ITIL fornisce le basi per ITSM.

gestione dei servizi IT (ITSM)

Attività associate alla progettazione, implementazione, gestione e supporto dei servizi IT per un'organizzazione. Per informazioni sull'integrazione delle operazioni cloud con gli strumenti ITSM, consulta la guida all'integrazione delle operazioni.

ITIL

Vedi la libreria di informazioni IT.

ITSM

Vedi Gestione dei servizi IT.

L

controllo degli accessi basato su etichette (LBAC)

Un'implementazione del controllo di accesso obbligatorio (MAC) in cui agli utenti e ai dati stessi viene assegnato esplicitamente un valore di etichetta di sicurezza. L'intersezione tra l'etichetta di sicurezza utente e l'etichetta di sicurezza dei dati determina quali righe e colonne possono essere visualizzate dall'utente.

zona di destinazione

Una landing zone è un AWS ambiente multi-account ben progettato, scalabile e sicuro. Questo è un punto di partenza dal quale le organizzazioni possono avviare e distribuire rapidamente carichi di lavoro e applicazioni con fiducia nel loro ambiente di sicurezza e infrastruttura. Per ulteriori informazioni sulle zone di destinazione, consulta la sezione Configurazione di un ambiente AWS multi-account sicuro e scalabile.

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi basato su etichette.

Privilegio minimo

La best practice di sicurezza per la concessione delle autorizzazioni minime richieste per eseguire un'attività. Per ulteriori informazioni, consulta Applicazione delle autorizzazioni del privilegio minimo nella documentazione di IAM.

eseguire il rehosting (lift and shift)

Vedi 7 R.

sistema little-endian

Un sistema che memorizza per primo il byte meno importante. Vedi anche endianità.

ambienti inferiori

Vedi ambiente.

M

machine learning (ML)

Un tipo di intelligenza artificiale che utilizza algoritmi e tecniche per il riconoscimento e l'apprendimento di schemi. Il machine learning analizza e apprende dai dati registrati, come i dati dell'Internet delle cose (IoT), per generare un modello statistico basato su modelli. Per ulteriori informazioni, consulta la sezione Machine learning.

ramo principale

Vedi filiale.

malware

Software progettato per compromettere la sicurezza o la privacy del computer. Il malware potrebbe interrompere i sistemi informatici, divulgare informazioni sensibili o ottenere accessi non autorizzati. Esempi di malware includono virus, worm, ransomware, trojan horse, spyware e keylogger.

servizi gestiti

AWS servizi per cui AWS gestisce il livello di infrastruttura, il sistema operativo e le piattaforme e si accede agli endpoint per archiviare e recuperare i dati. Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) e Amazon DynamoDB sono esempi di servizi gestiti. Questi sono noti anche come servizi astratti.

sistema di esecuzione della produzione (MES)

Un sistema software per tracciare, monitorare, documentare e controllare i processi di produzione che convertono le materie prime in prodotti finiti in officina.

MAP

Vedi Migration Acceleration Program.

meccanismo

Un processo completo in cui si crea uno strumento, si promuove l'adozione dello strumento e quindi si esaminano i risultati per apportare le modifiche. Un meccanismo è un ciclo che si rafforza e si migliora man mano che funziona. Per ulteriori informazioni, consulta Creazione di meccanismi nel AWS Well-Architected Framework.

account membro

Tutti gli account Account AWS diversi dall'account di gestione che fanno parte di un'organizzazione in. AWS Organizations Un account può essere membro di una sola organizzazione alla volta.

MEH

Vedi sistema di esecuzione della produzione.

Message Queuing Telemetry Transport (MQTT)

Un protocollo di comunicazione machine-to-machine (M2M) leggero, basato sul modello di pubblicazione/sottoscrizione, per dispositivi IoT con risorse limitate.

microservizio

Un piccolo servizio indipendente che comunica tramite API ben definite ed è in genere di proprietà di piccoli team autonomi. Ad esempio, un sistema assicurativo potrebbe includere microservizi che si riferiscono a funzionalità aziendali, come vendite o marketing, o sottodomini, come acquisti, reclami o analisi. I vantaggi dei microservizi includono agilità, dimensionamento flessibile, facilità di implementazione, codice riutilizzabile e resilienza. Per ulteriori informazioni, consulta Integrazione dei microservizi utilizzando servizi serverless. AWS

architettura di microservizi

Un approccio alla creazione di un'applicazione con componenti indipendenti che eseguono ogni processo applicativo come microservizio. Questi microservizi comunicano tramite un'interfaccia ben definita utilizzando API leggere. Ogni microservizio in questa architettura può essere aggiornato, distribuito e dimensionato per soddisfare la richiesta di funzioni specifiche di un'applicazione. Per ulteriori informazioni, vedere Implementazione dei microservizi su. AWS

Programma di accelerazione della migrazione (MAP)

Un AWS programma che fornisce consulenza, supporto, formazione e servizi per aiutare le organizzazioni a costruire una solida base operativa per il passaggio al cloud e per contribuire a compensare il costo iniziale delle migrazioni. MAP include una metodologia di migrazione per eseguire le migrazioni precedenti in modo metodico e un set di strumenti per automatizzare e accelerare gli scenari di migrazione comuni.

migrazione su larga scala

Il processo di trasferimento della maggior parte del portfolio di applicazioni sul cloud avviene a ondate, con più applicazioni trasferite a una velocità maggiore in ogni ondata. Questa fase utilizza le migliori pratiche e le lezioni apprese nelle fasi precedenti per implementare una fabbrica di migrazione di team, strumenti e processi per semplificare la migrazione dei carichi di lavoro attraverso l'automazione e la distribuzione agile. Questa è la terza fase della strategia di migrazione AWS.

fabbrica di migrazione

Team interfunzionali che semplificano la migrazione dei carichi di lavoro attraverso approcci automatizzati e agili. I team di Migration Factory includono in genere operazioni, analisti e proprietari aziendali, ingegneri addetti alla migrazione, sviluppatori e DevOps professionisti che lavorano nell'ambito degli sprint. Tra il 20% e il 50% di un portfolio di applicazioni aziendali è costituito da schemi ripetuti che possono essere ottimizzati con un approccio di fabbrica. Per ulteriori informazioni, consulta la discussione sulle fabbriche di migrazione e la Guida alla fabbrica di migrazione al cloud in questo set di contenuti.

metadati di migrazione

Le informazioni sull'applicazione e sul server necessarie per completare la migrazione. Ogni modello di migrazione richiede un set diverso di metadati di migrazione. Esempi di metadati di migrazione includono la sottorete, il gruppo di sicurezza e l'account di destinazione. AWS

modello di migrazione

Un'attività di migrazione ripetibile che descrive in dettaglio la strategia di migrazione, la destinazione della migrazione e l'applicazione o il servizio di migrazione utilizzati. Esempio: riorganizza la migrazione su Amazon EC2 AWS con Application Migration Service.

Valutazione del portfolio di migrazione (MPA)

Uno strumento online che fornisce informazioni per la convalida del business case per la migrazione a. Cloud AWS MPA offre una valutazione dettagliata del portfolio (dimensionamento

corretto dei server, prezzi, confronto del TCO, analisi dei costi di migrazione) e pianificazione della migrazione (analisi e raccolta dei dati delle applicazioni, raggruppamento delle applicazioni, prioritizzazione delle migrazioni e pianificazione delle ondate). Lo strumento MPA (richiede l'accesso) è disponibile gratuitamente per tutti i AWS consulenti e i consulenti dei partner APN.

valutazione della preparazione alla migrazione (MRA)

Il processo di acquisizione di informazioni sullo stato di preparazione al cloud di un'organizzazione, l'identificazione dei punti di forza e di debolezza e la creazione di un piano d'azione per colmare le lacune identificate, utilizzando il CAF. AWS Per ulteriori informazioni, consulta la guida di preparazione alla migrazione. MRA è la prima fase della strategia di migrazione AWS.

strategia di migrazione

L'approccio utilizzato per migrare un carico di lavoro verso. Cloud AWS Per ulteriori informazioni, consulta la voce 7 R in questo glossario e consulta Mobilita la tua organizzazione per accelerare le migrazioni su larga scala.

ML

Vedi machine learning.

modernizzazione

Trasformazione di un'applicazione obsoleta (legacy o monolitica) e della relativa infrastruttura in un sistema agile, elastico e altamente disponibile nel cloud per ridurre i costi, aumentare l'efficienza e sfruttare le innovazioni. Per ulteriori informazioni, vedere Strategia per la modernizzazione delle applicazioni in. Cloud AWS

valutazione della preparazione alla modernizzazione

Una valutazione che aiuta a determinare la preparazione alla modernizzazione delle applicazioni di un'organizzazione, identifica vantaggi, rischi e dipendenze e determina in che misura l'organizzazione può supportare lo stato futuro di tali applicazioni. Il risultato della valutazione è uno schema dell'architettura di destinazione, una tabella di marcia che descrive in dettaglio le fasi di sviluppo e le tappe fondamentali del processo di modernizzazione e un piano d'azione per colmare le lacune identificate. Per ulteriori informazioni, vedere Valutazione della preparazione alla modernizzazione per le applicazioni in. Cloud AWS

applicazioni monolitiche (monoliti)

Applicazioni eseguite come un unico servizio con processi strettamente collegati. Le applicazioni monolitiche presentano diversi inconvenienti. Se una funzionalità dell'applicazione registra un

picco di domanda, l'intera architettura deve essere dimensionata. L'aggiunta o il miglioramento delle funzionalità di un'applicazione monolitica diventa inoltre più complessa man mano che la base di codice cresce. Per risolvere questi problemi, puoi utilizzare un'architettura di microservizi. Per ulteriori informazioni, consulta la sezione Scomposizione dei monoliti in microservizi.

MAPPA

Vedi Migration Portfolio Assessment.

MQTT

Vedi Message Queuing Telemetry Transport.

classificazione multiclasse

Un processo che aiuta a generare previsioni per più classi (prevedendo uno o più di due risultati). Ad esempio, un modello di machine learning potrebbe chiedere "Questo prodotto è un libro, un'auto o un telefono?" oppure "Quale categoria di prodotti è più interessante per questo cliente?"

infrastruttura mutabile

Un modello che aggiorna e modifica l'infrastruttura esistente per i carichi di lavoro di produzione. Per migliorare la coerenza, l'affidabilità e la prevedibilità, il AWS Well-Architected Framework consiglia l'uso di un'infrastruttura immutabile come best practice.

O

OAC

Vedi Origin Access Control.

QUERCIA

Vedi Origin Access Identity.

OCM

Vedi gestione delle modifiche organizzative.

migrazione offline

Un metodo di migrazione in cui il carico di lavoro di origine viene eliminato durante il processo di migrazione. Questo metodo prevede tempi di inattività prolungati e viene in genere utilizzato per carichi di lavoro piccoli e non critici.

OI

Vedi l'integrazione delle operazioni.

OLA

Vedi accordo a livello operativo.

migrazione online

Un metodo di migrazione in cui il carico di lavoro di origine viene copiato sul sistema di destinazione senza essere messo offline. Le applicazioni connesse al carico di lavoro possono continuare a funzionare durante la migrazione. Questo metodo comporta tempi di inattività pari a zero o comunque minimi e viene in genere utilizzato per carichi di lavoro di produzione critici.

OPC-UA

Vedi Open Process Communications - Unified Architecture.

Comunicazioni a processo aperto - Architettura unificata (OPC-UA)

Un protocollo di comunicazione machine-to-machine (M2M) per l'automazione industriale. OPC-UA fornisce uno standard di interoperabilità con schemi di crittografia, autenticazione e autorizzazione dei dati.

accordo a livello operativo (OLA)

Un accordo che chiarisce quali sono gli impegni reciproci tra i gruppi IT funzionali, a supporto di un accordo sul livello di servizio (SLA).

revisione della prontezza operativa (ORR)

Un elenco di domande e best practice associate che aiutano a comprendere, valutare, prevenire o ridurre la portata degli incidenti e dei possibili guasti. Per ulteriori informazioni, vedere Operational Readiness Reviews (ORR) nel Well-Architected AWS Framework.

tecnologia operativa (OT)

Sistemi hardware e software che interagiscono con l'ambiente fisico per controllare le operazioni, le apparecchiature e le infrastrutture industriali. Nella produzione, l'integrazione di sistemi OT e di tecnologia dell'informazione (IT) è un obiettivo chiave per le trasformazioni dell'Industria 4.0.

integrazione delle operazioni (OI)

Il processo di modernizzazione delle operazioni nel cloud, che prevede la pianificazione, l'automazione e l'integrazione della disponibilità. Per ulteriori informazioni, consulta la guida all'integrazione delle operazioni.

trail organizzativo

Un percorso creato da noi AWS CloudTrail che registra tutti gli eventi di un'organizzazione per tutti Account AWS . AWS Organizations Questo percorso viene creato in ogni Account AWS che fa parte dell'organizzazione e tiene traccia dell'attività in ogni account. Per ulteriori informazioni, consulta Creazione di un percorso per un'organizzazione nella CloudTrail documentazione.

gestione del cambiamento organizzativo (OCM)

Un framework per la gestione di trasformazioni aziendali importanti e che comportano l'interruzione delle attività dal punto di vista delle persone, della cultura e della leadership. OCM aiuta le organizzazioni a prepararsi e passare a nuovi sistemi e strategie accelerando l'adozione del cambiamento, affrontando i problemi di transizione e promuovendo cambiamenti culturali e organizzativi. Nella strategia di AWS migrazione, questo framework si chiama accelerazione delle persone, a causa della velocità di cambiamento richiesta nei progetti di adozione del cloud. Per ulteriori informazioni, consultare la Guida OCM.

controllo dell'accesso all'origine (OAC)

In CloudFront, un'opzione avanzata per limitare l'accesso per proteggere i contenuti di Amazon Simple Storage Service (Amazon S3). OAC supporta tutti i bucket S3 in generale Regioni AWS, la crittografia lato server con AWS KMS (SSE-KMS) e le richieste dinamiche e dirette al bucket S3. `PUT` `DELETE`

identità di accesso origine (OAI)

Nel CloudFront, un'opzione per limitare l'accesso per proteggere i tuoi contenuti Amazon S3. Quando usi OAI, CloudFront crea un principale con cui Amazon S3 può autenticarsi. I principali autenticati possono accedere ai contenuti in un bucket S3 solo tramite una distribuzione specifica. CloudFront Vedi anche OAC, che fornisce un controllo degli accessi più granulare e avanzato.

O

Vedi la revisione della prontezza operativa.

- NON

Vedi la tecnologia operativa.

VPC in uscita (egress)

In un'architettura AWS multi-account, un VPC che gestisce le connessioni di rete avviate dall'interno di un'applicazione. Nel documento Architettura di riferimento per la sicurezza di

AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

P

limite delle autorizzazioni

Una policy di gestione IAM collegata ai principali IAM per impostare le autorizzazioni massime che l'utente o il ruolo possono avere. Per ulteriori informazioni, consulta Limiti delle autorizzazioni nella documentazione di IAM.

informazioni di identificazione personale (PII)

Informazioni che, se visualizzate direttamente o abbinate ad altri dati correlati, possono essere utilizzate per dedurre ragionevolmente l'identità di un individuo. Esempi di informazioni personali includono nomi, indirizzi e informazioni di contatto.

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

Una serie di passaggi predefiniti che raccolgono il lavoro associato alle migrazioni, come l'erogazione delle funzioni operative principali nel cloud. Un playbook può assumere la forma di script, runbook automatici o un riepilogo dei processi o dei passaggi necessari per gestire un ambiente modernizzato.

PLC

Vedi controllore logico programmabile.

PLM

Vedi la gestione del ciclo di vita del prodotto.

policy

Un oggetto in grado di definire le autorizzazioni (vedi politica basata sull'identità), specificare le condizioni di accesso (vedi politicabasata sulle risorse) o definire le autorizzazioni massime per tutti gli account di un'organizzazione in (vedi politica di controllo dei servizi). AWS Organizations

persistenza poliglotta

Scelta indipendente della tecnologia di archiviazione di dati di un microservizio in base ai modelli di accesso ai dati e ad altri requisiti. Se i microservizi utilizzano la stessa tecnologia di archiviazione di dati, possono incontrare problemi di implementazione o registrare prestazioni scadenti. I microservizi vengono implementati più facilmente e ottengono prestazioni e scalabilità migliori se utilizzano l'archivio dati più adatto alle loro esigenze. Per ulteriori informazioni, consulta la sezione Abilitazione della persistenza dei dati nei microservizi.

valutazione del portfolio

Un processo di scoperta, analisi e definizione delle priorità del portfolio di applicazioni per pianificare la migrazione. Per ulteriori informazioni, consulta la pagina Valutazione della preparazione alla migrazione.

predicate

Una condizione di interrogazione che restituisce o, in genere, si trova in una clausola`true`. `false` `WHERE`

predicato pushdown

Una tecnica di ottimizzazione delle query del database che filtra i dati della query prima del trasferimento. Ciò riduce la quantità di dati che devono essere recuperati ed elaborati dal database relazionale e migliora le prestazioni delle query.

controllo preventivo

Un controllo di sicurezza progettato per impedire il verificarsi di un evento. Questi controlli sono la prima linea di difesa per impedire accessi non autorizzati o modifiche indesiderate alla rete. Per ulteriori informazioni, consulta Controlli preventivi in Implementazione dei controlli di sicurezza in AWS.

principale

Un'entità in AWS grado di eseguire azioni e accedere alle risorse. Questa entità è in genere un utente root per un Account AWS ruolo IAM o un utente. Per ulteriori informazioni, consulta Principali in Termini e concetti dei ruoli nella documentazione di IAM.

Privacy fin dalla progettazione

Un approccio all'ingegneria dei sistemi che tiene conto della privacy durante l'intero processo di progettazione.

zone ospitate private

Un container che contiene informazioni su come si desidera che Amazon Route 53 risponda alle query DNS per un dominio e i relativi sottodomini all'interno di uno o più VPC. Per ulteriori informazioni, consulta Utilizzo delle zone ospitate private nella documentazione di Route 53.

controllo proattivo

Un controllo di sicurezza progettato per impedire l'implementazione di risorse non conformi. Questi controlli analizzano le risorse prima del loro provisioning. Se la risorsa non è conforme al controllo, non viene fornita. Per ulteriori informazioni, consulta la guida di riferimento sui controlli nella AWS Control Tower documentazione e consulta Controlli proattivi in Implementazione dei controlli di sicurezza su. AWS

gestione del ciclo di vita del prodotto (PLM)

La gestione dei dati e dei processi di un prodotto durante l'intero ciclo di vita, dalla progettazione, sviluppo e lancio, attraverso la crescita e la maturità, fino al declino e alla rimozione.

Ambiente di produzione

Vedi ambiente.

controllore logico programmabile (PLC)

Nella produzione, un computer altamente affidabile e adattabile che monitora le macchine e automatizza i processi di produzione.

pseudonimizzazione

Il processo di sostituzione degli identificatori personali in un set di dati con valori segnaposto. La pseudonimizzazione può aiutare a proteggere la privacy personale. I dati pseudonimizzati sono ancora considerati dati personali.

pubblica/sottoscrivi (pub/sub)

Un pattern che consente comunicazioni asincrone tra microservizi per migliorare la scalabilità e la reattività. Ad esempio, in un MES basato su microservizi, un microservizio può pubblicare messaggi di eventi su un canale a cui altri microservizi possono abbonarsi. Il sistema può aggiungere nuovi microservizi senza modificare il servizio di pubblicazione.

Q

Piano di query

Una serie di passaggi, come le istruzioni, utilizzati per accedere ai dati in un sistema di database relazionale SQL.

regressione del piano di query

Quando un ottimizzatore del servizio di database sceglie un piano non ottimale rispetto a prima di una determinata modifica all'ambiente di database. Questo può essere causato da modifiche a statistiche, vincoli, impostazioni dell'ambiente, associazioni dei parametri di query e aggiornamenti al motore di database.

R

Matrice RACI

Vedi responsabile, responsabile, consultato, informato (RACI).

ransomware

Un software dannoso progettato per bloccare l'accesso a un sistema informatico o ai dati fino a quando non viene effettuato un pagamento.

Matrice RASCI

Vedi responsabile, responsabile, consultato, informato (RACI).

RCAC

Vedi controllo dell'accesso a righe e colonne.

replica di lettura

Una copia di un database utilizzata per scopi di sola lettura. È possibile indirizzare le query alla replica di lettura per ridurre il carico sul database principale.

riprogettare

Vedi 7 Rs.

obiettivo del punto di ripristino (RPO)

Il periodo di tempo massimo accettabile dall'ultimo punto di ripristino dei dati. Ciò determina quella che viene considerata una perdita di dati accettabile tra l'ultimo punto di ripristino e l'interruzione del servizio.

obiettivo del tempo di ripristino (RTO)

Il ritardo massimo accettabile tra l'interruzione del servizio e il ripristino del servizio.

rifattorizzare

Vedi 7 R.

Regione

Una raccolta di AWS risorse in un'area geografica. Ciascuna Regione AWS è isolata e indipendente dalle altre per fornire tolleranza agli errori, stabilità e resilienza. Per ulteriori informazioni, consulta Specificare cosa può usare Regioni AWS il tuo account.

regressione

Una tecnica di ML che prevede un valore numerico. Ad esempio, per risolvere il problema "A che prezzo verrà venduta questa casa?" un modello di ML potrebbe utilizzare un modello di regressione lineare per prevedere il prezzo di vendita di una casa sulla base di dati noti sulla casa (ad esempio, la metratura).

riospitare

Vedi 7 R.

rilascio

In un processo di implementazione, l'atto di promuovere modifiche a un ambiente di produzione.

trasferisco

Vedi 7 Rs.

ripiattaforma

Vedi 7 Rs.

riacquisto

Vedi 7 Rs.

resilienza

La capacità di un'applicazione di resistere o ripristinare le interruzioni. L'elevata disponibilità e il disaster recovery sono considerazioni comuni quando si pianifica la resilienza in. Cloud AWSPer ulteriori informazioni, vedere Cloud AWS Resilience.

policy basata su risorse

Una policy associata a una risorsa, ad esempio un bucket Amazon S3, un endpoint o una chiave di crittografia. Questo tipo di policy specifica a quali principali è consentito l'accesso, le azioni supportate e qualsiasi altra condizione che deve essere soddisfatta.

matrice di assegnazione di responsabilità (RACI)

Una matrice che definisce i ruoli e le responsabilità di tutte le parti coinvolte nelle attività di migrazione e nelle operazioni cloud. Il nome della matrice deriva dai tipi di responsabilità definiti nella matrice: responsabile (R), responsabile (A), consultato (C) e informato (I). Il tipo di supporto (S) è facoltativo. Se includi il supporto, la matrice viene chiamata matrice RASCI e, se la escludi, viene chiamata matrice RACI.

controllo reattivo

Un controllo di sicurezza progettato per favorire la correzione di eventi avversi o deviazioni dalla baseline di sicurezza. Per ulteriori informazioni, consulta Controlli reattivi in Implementazione dei controlli di sicurezza in AWS.

retain

Vedi 7 R.

andare in pensione

Vedi 7 Rs.

rotazione

Processo di aggiornamento periodico di un segreto per rendere più difficile l'accesso alle credenziali da parte di un utente malintenzionato.

controllo dell'accesso a righe e colonne (RCAC)

L'uso di espressioni SQL di base e flessibili con regole di accesso definite. RCAC è costituito da autorizzazioni di riga e maschere di colonna.

RPO

Vedi l'obiettivo del punto di ripristino.

RTO

Vedi l'obiettivo del tempo di ripristino.

runbook

Un insieme di procedure manuali o automatizzate necessarie per eseguire un'attività specifica. In genere sono progettati per semplificare operazioni o procedure ripetitive con tassi di errore elevati.

S

SAML 2.0

Uno standard aperto utilizzato da molti provider di identità (IdPs). Questa funzionalità abilita il single sign-on (SSO) federato, in modo che gli utenti possano accedere AWS Management Console o chiamare le operazioni AWS API senza che tu debba creare un utente in IAM per tutti i membri dell'organizzazione. Per ulteriori informazioni sulla federazione basata su SAML 2.0, consulta Informazioni sulla federazione basata su SAML 2.0 nella documentazione di IAM.

SCADA

Vedi controllo di supervisione e acquisizione dati.

SCP

Vedi la politica di controllo del servizio.

Secret

In AWS Secrets Manager, informazioni riservate o riservate, come una password o le credenziali utente, archiviate in forma crittografata. È costituito dal valore segreto e dai relativi metadati. Il valore segreto può essere binario, una stringa singola o più stringhe. Per ulteriori informazioni, consulta Cosa c'è in un segreto di Secrets Manager? nella documentazione di Secrets Manager.

controllo di sicurezza

Un guardrail tecnico o amministrativo che impedisce, rileva o riduce la capacità di un autore di minacce di sfruttare una vulnerabilità di sicurezza. Esistono quattro tipi principali di controlli di sicurezza: preventivi, investigativi, reattivi e proattivi.

rafforzamento della sicurezza

Il processo di riduzione della superficie di attacco per renderla più resistente agli attacchi. Può includere azioni come la rimozione di risorse che non sono più necessarie, l'implementazione di

best practice di sicurezza che prevedono la concessione del privilegio minimo o la disattivazione di funzionalità non necessarie nei file di configurazione.

sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM)

Strumenti e servizi che combinano sistemi di gestione delle informazioni di sicurezza (SIM) e sistemi di gestione degli eventi di sicurezza (SEM). Un sistema SIEM raccoglie, monitora e analizza i dati da server, reti, dispositivi e altre fonti per rilevare minacce e violazioni della sicurezza e generare avvisi.

automazione della risposta alla sicurezza

Un'azione predefinita e programmata progettata per rispondere o porre rimedio automaticamente a un evento di sicurezza. Queste automazioni fungono da controlli di sicurezza investigativi o reattivi che aiutano a implementare le migliori pratiche di sicurezza. AWS Esempi di azioni di risposta automatizzate includono la modifica di un gruppo di sicurezza VPC, l'applicazione di patch a un'istanza Amazon EC2 o la rotazione delle credenziali.

Crittografia lato server

Crittografia dei dati a destinazione, da parte di chi li riceve. AWS servizio

Policy di controllo dei servizi (SCP)

Una policy che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in AWS Organizations. Le SCP definiscono i guardrail o fissano i limiti alle azioni che un amministratore può delegare a utenti o ruoli. Puoi utilizzare le SCP come elenchi consentiti o elenchi di rifiuto, per specificare quali servizi o azioni sono consentiti o proibiti. Per ulteriori informazioni, consulta le politiche di controllo del servizio nella AWS Organizations documentazione.

endpoint del servizio

L'URL del punto di ingresso per un AWS servizio. Puoi utilizzare l'endpoint per connetterti a livello di programmazione al servizio di destinazione. Per ulteriori informazioni, consulta Endpoint del AWS servizio nei Riferimenti generali di AWS.

accordo sul livello di servizio (SLA)

Un accordo che chiarisce ciò che un team IT promette di offrire ai propri clienti, ad esempio l'operatività e le prestazioni del servizio.

indicatore del livello di servizio (SLI)

Misurazione di un aspetto prestazionale di un servizio, ad esempio il tasso di errore, la disponibilità o la velocità effettiva.

obiettivo a livello di servizio (SLO)

Una metrica target che rappresenta lo stato di un servizio, misurato da un indicatore del livello di servizio.

Modello di responsabilità condivisa

Un modello che descrive la responsabilità condivisa AWS per la sicurezza e la conformità del cloud. AWS è responsabile della sicurezza del cloud, mentre tu sei responsabile della sicurezza nel cloud. Per ulteriori informazioni, consulta Modello di responsabilità condivisa.

SIEM

Vedi il sistema di gestione delle informazioni e degli eventi sulla sicurezza.

punto di errore singolo (SPOF)

Un guasto in un singolo componente critico di un'applicazione che può disturbare il sistema.

SLAM

Vedi il contratto sul livello di servizio.

SLI

Vedi l'indicatore del livello di servizio.

LENTA

Vedi obiettivo del livello di servizio.

split-and-seed modello

Un modello per dimensionare e accelerare i progetti di modernizzazione. Man mano che vengono definite nuove funzionalità e versioni dei prodotti, il team principale si divide per creare nuovi team di prodotto. Questo aiuta a dimensionare le capacità e i servizi dell'organizzazione, migliora la produttività degli sviluppatori e supporta una rapida innovazione. Per ulteriori informazioni, vedere Approccio graduale alla modernizzazione delle applicazioni in. Cloud AWS

SPOF

Vedi punto di errore singolo.

schema a stella

Una struttura organizzativa di database che utilizza un'unica tabella dei fatti di grandi dimensioni per archiviare i dati transazionali o misurati e utilizza una o più tabelle dimensionali più piccole per memorizzare gli attributi dei dati. Questa struttura è progettata per l'uso in un data warehouse o per scopi di business intelligence.

modello del fico strangolatore

Un approccio alla modernizzazione dei sistemi monolitici mediante la riscrittura e la sostituzione incrementali delle funzionalità del sistema fino alla disattivazione del sistema legacy. Questo modello utilizza l'analogia di una pianta di fico che cresce fino a diventare un albero robusto e alla fine annienta e sostituisce il suo ospite. Il modello è stato introdotto da Martin Fowler come metodo per gestire il rischio durante la riscrittura di sistemi monolitici. Per un esempio di come applicare questo modello, consulta Modernizzazione incrementale dei servizi Web legacy di Microsoft ASP.NET (ASMX) mediante container e Gateway Amazon API.

sottorete

Un intervallo di indirizzi IP nel VPC. Una sottorete deve risiedere in una singola zona di disponibilità.

controllo di supervisione e acquisizione dati (SCADA)

Nella produzione, un sistema che utilizza hardware e software per monitorare gli asset fisici e le operazioni di produzione.

crittografia simmetrica

Un algoritmo di crittografia che utilizza la stessa chiave per crittografare e decrittografare i dati.

test sintetici

Test di un sistema in modo da simulare le interazioni degli utenti per rilevare potenziali problemi o monitorare le prestazioni. Puoi usare Amazon CloudWatch Synthetics per creare questi test.

T

tags

Coppie chiave-valore che fungono da metadati per l'organizzazione delle risorse. AWS Con i tag è possibile a gestire, identificare, organizzare, cercare e filtrare le risorse. Per ulteriori informazioni, consulta Tagging delle risorse AWS.

variabile di destinazione

Il valore che stai cercando di prevedere nel machine learning supervisionato. Questo è indicato anche come variabile di risultato. Ad esempio, in un ambiente di produzione la variabile di destinazione potrebbe essere un difetto del prodotto.

elenco di attività

Uno strumento che viene utilizzato per tenere traccia dei progressi tramite un runbook. Un elenco di attività contiene una panoramica del runbook e un elenco di attività generali da completare. Per ogni attività generale, include la quantità stimata di tempo richiesta, il proprietario e lo stato di avanzamento.

Ambiente di test

Vedi ambiente.

training

Fornire dati da cui trarre ispirazione dal modello di machine learning. I dati di training devono contenere la risposta corretta. L'algoritmo di apprendimento trova nei dati di addestramento i pattern che mappano gli attributi dei dati di input al target (la risposta che si desidera prevedere). Produce un modello di ML che acquisisce questi modelli. Puoi quindi utilizzare il modello di ML per creare previsioni su nuovi dati di cui non si conosce il target.

Transit Gateway

Un hub di transito di rete che è possibile utilizzare per collegare i VPC e le reti on-premise. Per ulteriori informazioni, consulta Cos'è un gateway di transito nella AWS Transit Gateway documentazione.

flusso di lavoro basato su trunk

Un approccio in cui gli sviluppatori creano e testano le funzionalità localmente in un ramo di funzionalità e quindi uniscono tali modifiche al ramo principale. Il ramo principale viene quindi integrato negli ambienti di sviluppo, preproduzione e produzione, in sequenza.

Accesso attendibile

Concessione delle autorizzazioni a un servizio specificato dall'utente per eseguire attività all'interno dell'organizzazione AWS Organizations e nei suoi account per conto dell'utente. Il servizio attendibile crea un ruolo collegato al servizio in ogni account, quando tale ruolo è necessario, per eseguire attività di gestione per conto dell'utente. Per ulteriori informazioni,

consulta Utilizzo AWS Organizations con altri AWS servizi nella AWS Organizations documentazione.

regolazione

Modificare alcuni aspetti del processo di training per migliorare la precisione del modello di ML. Ad esempio, puoi addestrare il modello di ML generando un set di etichette, aggiungendo etichette e quindi ripetendo questi passaggi più volte con impostazioni diverse per ottimizzare il modello.

team da due pizze

Una piccola DevOps squadra che puoi sfamare con due pizze. Un team composto da due persone garantisce la migliore opportunità possibile di collaborazione nello sviluppo del software.

U

incertezza

Un concetto che si riferisce a informazioni imprecise, incomplete o sconosciute che possono minare l'affidabilità dei modelli di machine learning predittivi. Esistono due tipi di incertezza: l'incertezza epistemica, che è causata da dati limitati e incompleti, mentre l'incertezza aleatoria è causata dal rumore e dalla casualità insiti nei dati. Per ulteriori informazioni, consulta la guida Quantificazione dell'incertezza nei sistemi di deep learning.

compiti indifferenziati

Conosciuto anche come sollevamento di carichi pesanti, è un lavoro necessario per creare e far funzionare un'applicazione, ma che non apporta valore diretto all'utente finale né offre vantaggi competitivi. Esempi di attività indifferenziate includono l'approvvigionamento, la manutenzione e la pianificazione della capacità.

ambienti superiori

Vedi ambiente.

V

vacuum

Un'operazione di manutenzione del database che prevede la pulizia dopo aggiornamenti incrementali per recuperare lo spazio di archiviazione e migliorare le prestazioni.

controllo delle versioni

Processi e strumenti che tengono traccia delle modifiche, ad esempio le modifiche al codice di origine in un repository.

Peering VPC

Una connessione tra due VPC che consente di instradare il traffico tramite indirizzi IP privati. Per ulteriori informazioni, consulta Che cos'è il peering VPC? nella documentazione di Amazon VPC.

vulnerabilità

Un difetto software o hardware che compromette la sicurezza del sistema.

W

cache calda

Una cache del buffer che contiene dati correnti e pertinenti a cui si accede frequentemente. L'istanza di database può leggere dalla cache del buffer, il che richiede meno tempo rispetto alla lettura dalla memoria dal disco principale.

dati caldi

Dati a cui si accede raramente. Quando si eseguono interrogazioni di questo tipo di dati, in genere sono accettabili interrogazioni moderatamente lente.

funzione finestra

Una funzione SQL che esegue un calcolo su un gruppo di righe che si riferiscono in qualche modo al record corrente. Le funzioni della finestra sono utili per l'elaborazione di attività, come il calcolo di una media mobile o l'accesso al valore delle righe in base alla posizione relativa della riga corrente.

Carico di lavoro

Una raccolta di risorse e codice che fornisce valore aziendale, ad esempio un'applicazione rivolta ai clienti o un processo back-end.

flusso di lavoro

Gruppi funzionali in un progetto di migrazione responsabili di una serie specifica di attività. Ogni flusso di lavoro è indipendente ma supporta gli altri flussi di lavoro del progetto. Ad esempio,

il flusso di lavoro del portfolio è responsabile della definizione delle priorità delle applicazioni, della pianificazione delle ondate e della raccolta dei metadati di migrazione. Il flusso di lavoro del portfolio fornisce queste risorse al flusso di lavoro di migrazione, che quindi migra i server e le applicazioni.

VERME

Vedi scrivere una volta, leggere molti.

WQF

Vedi AWS Workload Qualification Framework.

scrivi una volta, leggi molte (WORM)

Un modello di storage che scrive i dati una sola volta e ne impedisce l'eliminazione o la modifica. Gli utenti autorizzati possono leggere i dati tutte le volte che è necessario, ma non possono modificarli. Questa infrastruttura di archiviazione dei dati è considerata immutabile.

Z

exploit zero-day

Un attacco, in genere malware, che sfrutta una vulnerabilità zero-day.

vulnerabilità zero-day

Un difetto o una vulnerabilità assoluta in un sistema di produzione. Gli autori delle minacce possono utilizzare questo tipo di vulnerabilità per attaccare il sistema. Gli sviluppatori vengono spesso a conoscenza della vulnerabilità causata dall'attacco.

applicazione zombie

Un'applicazione che prevede un utilizzo CPU e memoria inferiore al 5%. In un progetto di migrazione, è normale ritirare queste applicazioni.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.