AWS Security Reference Architecture (AWS SRA): architettura di base

AWS Guida prescrittiva

AWS Guida prescrittiva: AWS Security Reference Architecture (AWS SRA): architettura di base

Table of Contents

AWS Security Reference Architecture (AWS SRA): architettura di base

Team di sicurezza dei servizi globali, Amazon Web Services (collaboratori)

Dicembre 2025 (cronologia dei documenti)

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

L'Amazon Web Services (AWS) Security Reference Architecture (AWS SRA) è un set olistico di linee guida per l'implementazione della gamma completa di servizi di AWS sicurezza in un ambiente multi-account. Usalo per aiutare a progettare, implementare e gestire i servizi di AWS sicurezza in modo che si allineino alle pratiche consigliate. AWS Le raccomandazioni si basano su un'architettura a pagina singola che include i servizi di AWS sicurezza: come aiutano a raggiungere gli obiettivi di sicurezza, dove possono essere implementati e gestiti al meglio nell'azienda e come interagiscono con altri servizi di sicurezza. Account AWSQuesta guida generale sull'architettura integra raccomandazioni dettagliate e specifiche dei servizi, come quelle disponibili sul sito Web della documentazione sulla sicurezza.AWS

L'architettura e i consigli di accompagnamento si basano sulle nostre esperienze collettive con i clienti aziendali. AWS Questo documento è un riferimento, una serie completa di linee guida da utilizzare per Servizi AWS proteggere un ambiente particolare, e i modelli di soluzione nel repository di codice AWS SRA sono stati progettati per l'architettura specifica illustrata in questo riferimento. Ogni cliente avrà esigenze diverse. Di conseguenza, la progettazione dell' AWS ambiente potrebbe differire dagli esempi forniti qui. Dovrete modificare e adattare questi consigli per adattarli al vostro ambiente individuale e alle vostre esigenze di sicurezza. In tutto il documento, ove appropriato, suggeriamo opzioni per scenari alternativi più frequenti.

L' AWS SRA è un insieme di linee guida in evoluzione e viene aggiornato periodicamente in base alle nuove versioni di servizi e funzionalità, al feedback dei clienti e al panorama delle minacce in continua evoluzione. Ogni aggiornamento includerà la data di revisione e il registro delle modifiche associato.

Sebbene ci basiamo su un diagramma di una pagina come base, l'architettura è più profonda di un singolo diagramma a blocchi e deve essere costruita su una base ben strutturata di fondamenti e

principi di sicurezza. È possibile utilizzare questo documento in due modi: come narrazione o come riferimento. Gli argomenti sono organizzati come una storia, quindi puoi leggerli dall'inizio (guida di base sulla sicurezza) alla fine (discussione degli esempi di codice che puoi implementare). In alternativa, puoi sfogliare il documento per concentrarti sui principi di sicurezza, i servizi, i tipi di account, le linee guida e gli esempi più pertinenti alle tue esigenze.

Questo documento è suddiviso nelle seguenti sezioni e in un'appendice:

- Informazioni sulla libreria AWS SRA fornisce una panoramica delle linee guida tecniche e del codice inclusi nella raccolta di pubblicazioni AWS SRA.
- Il valore della AWS SRA illustra le motivazioni alla base della creazione della AWS SRA, descrive come utilizzarla per migliorare la sicurezza ed elenca i punti chiave.
- Security Foundations esamina il AWS Cloud Adoption Framework (AWS CAF), il AWS Well-Architected Framework e AWS il modello di responsabilità condivisa ed evidenzia gli elementi particolarmente rilevanti per l'SRA. AWS
- AWS Organizations, accounts e IAM guardrails introducono il AWS Organizations servizio, illustrano le funzionalità e i guardrails di sicurezza fondamentali e forniscono una panoramica della nostra strategia multi-account consigliata.
- La AWS Security Reference Architecture è un diagramma di architettura a pagina singola che mostra i servizi e le funzionalità e le funzionalità funzionali e di sicurezza Account AWS generalmente disponibili.
- AI/ML for security descrive in che modo diversi Servizi AWS utilizzano l'intelligenza artificiale e l'apprendimento automatico (AI/ML) in background per aiutarvi a raggiungere obiettivi di sicurezza specifici. Puoi includerli Servizi AWS nel tuo progetto per sfruttare le funzionalità di sicurezza avanzate.
- Creazione dell'architettura di sicurezza – Un approccio graduale fornisce indicazioni su come creare un'architettura di sicurezza personalizzata in sei fasi iterative, sulla base del riferimento fornito dall' AWS SRA.
- AWS L'elenco di controllo delle migliori pratiche SRA riassume le raccomandazioni illustrate nella guida in una lista di controllo che è possibile seguire durante la creazione della versione dell'architettura di sicurezza.
- Le risorse IAM presentano un riepilogo e una serie di indicazioni AWS Identity and Access Management (IAM) importanti per la vostra architettura di sicurezza.
- Code repository for AWS SRA examples fornisce una panoramica del GitHub repository associato che aiuterà sviluppatori e ingegneri a implementare alcune delle linee guida e dei modelli di

architettura presentati in questo documento. È possibile distribuire gli esempi utilizzando o Terraform by. AWS CloudFormation HashiCorp Supportano entrambi gli ambienti AWS Control Tower e quelli non AWS Control Tower .

L'appendice contiene un elenco dei singoli servizi di AWS sicurezza, identità e conformità e fornisce collegamenti a ulteriori informazioni su ciascun servizio. La sezione Cronologia dei documenti fornisce un registro delle modifiche per tenere traccia delle versioni di questo documento. Puoi anche iscriverti a un feed RSS per le notifiche di modifica.

Informazioni sulla libreria AWS SRA

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

Questa guida fa parte di una libreria che fornisce modelli architettonici e linee guida tecniche per la progettazione e la creazione di architetture di sicurezza. AWS La libreria è composta da codice di implementazione (libreria di codici AWS SRA), uno strumento di convalida (SRA Verify) e due categorie complementari di guide che coprono l'architettura di base e le architetture di deep dive.

AWS SRA: architettura di base (questa guida)

Questa guida rappresenta una base per l'architettura di AWS sicurezza consigliata. È il punto di partenza che si applica a tutte le organizzazioni, indipendentemente dal settore, dal tipo di applicazione o da qualsiasi altra considerazione. Questa base ti aiuta a costruire un'architettura solida e scalabile AWS e a creare una solida base di sicurezza AWS multi-account che si adatta in modo sicuro man mano che la tua azienda cresce.

AWS SRA: architetture deep dive

La guida all'architettura di base AWS SRA è completata da pubblicazioni aggiuntive che forniscono modelli architettonici allineati a funzionalità di sicurezza specifiche, tipi di applicazioni e requisiti di conformità o normativi. Questi modelli estendono l'architettura di base e devono essere utilizzati insieme alla AWS SRA — guida all'architettura di base.

Le seguenti guide forniscono modelli architettonici allineati a funzionalità di sicurezza specifiche:

- AWS SRA — identity management fornisce indicazioni su come implementare una soluzione scalabile, robusta e centralizzata per la gestione delle identità e degli accessi. AWS
- AWS SRA: la sicurezza perimetrale illustra i modelli di architettura e Servizi AWS l'implementazione della sicurezza perimetrale in un account centrale o in singoli account.
- AWS SRA — cyber forensics descrive come configurare un account AWS Forensics come punto di partenza per sviluppare le capacità forensi dell'organizzazione e contribuire a migliorare la preparazione alla risposta agli incidenti di sicurezza (IR).

Le seguenti guide forniscono modelli architettonici per tipi di applicazioni specifici. Potresti concentrarti su questi dopo aver creato la tua architettura di sicurezza di base:

- AWS SRA — AI Security fornisce consigli sull'architettura di sicurezza per la progettazione e la creazione di applicazioni che incorporano funzionalità di intelligenza artificiale generativa utilizzando servizi di intelligenza artificiale AWS generativa.
- AWS SRA — IoT fornisce consigli sull' AWS architettura di sicurezza per la progettazione e la creazione di applicazioni IoT.

Inoltre, la seguente guida descrive i modelli architettonici allineati a specifici quadri normativi o di conformità:

- AWS La Privacy Reference Architecture (AWS PRA) fornisce un'architettura di sicurezza per le applicazioni che trattano dati personali e deve supportare ampi requisiti di conformità in materia di privacy, come il Regolamento generale sulla protezione dei dati (GDPR), il California Consumer Privacy Act (CCPA) o la Legge generale sulla protezione dei dati (LGPD) del Brasile. Il AWS PRA fornisce una serie di linee guida specifiche per la progettazione e la configurazione dei controlli sulla privacy in. Servizi AWS

Ti consigliamo di iniziare con la AWS SRA — guida all'architettura di base per comprendere l'architettura di base e quindi di consultare le guide complementari per sfruttare funzionalità e implementazioni avanzate. Per ulteriori informazioni su questo set di contenuti, consulta AWS Security Reference Architecture.

> **Diagrammi di architettura**
>
> Per personalizzare i diagrammi dell'architettura di riferimento nella libreria AWS SRA in base alle esigenze aziendali, è possibile scaricare il seguente file.zip ed estrarne il contenuto.
>
> Scarica il file sorgente del diagramma (PowerPointformato Microsoft)

Il valore della AWS SRA

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

AWS dispone di un ampio (e crescente) set di servizi di sicurezza e relativi alla sicurezza. I clienti hanno espresso apprezzamento per le informazioni dettagliate disponibili attraverso la documentazione di servizio, i post di blog, i tutorial, i summit e le conferenze. Ci dicono anche che vogliono comprendere meglio il quadro generale e avere una visione strategica dei servizi di sicurezza. AWS Quando collaboriamo con i clienti per comprendere meglio ciò di cui hanno bisogno, emergono tre priorità:

- I clienti desiderano maggiori informazioni e modelli consigliati su come implementare, configurare e gestire i servizi di AWS sicurezza in modo olistico. In quali account e verso quali obiettivi di sicurezza devono essere distribuiti e gestiti i servizi? Esiste un account di sicurezza in cui devono funzionare tutti o la maggior parte dei servizi? In che modo la scelta della sede (unità organizzativa o Account AWS) influisce sugli obiettivi di sicurezza? Di quali compromessi (considerazioni di progettazione) i clienti devono essere consapevoli?
- I clienti sono interessati a vedere prospettive diverse per l'organizzazione logica dei numerosi servizi di sicurezza. AWS Oltre alla funzione principale di ogni servizio (ad esempio, servizi di identità o servizi di registrazione), questi punti di vista alternativi aiutano i clienti a pianificare, progettare e implementare la propria architettura di sicurezza. Un esempio condiviso più avanti in questo documento raggruppa i servizi in base ai livelli di protezione allineati alla struttura consigliata dell'ambiente. AWS
- I clienti sono alla ricerca di indicazioni ed esempi per integrare i servizi di sicurezza nel modo più efficace. Ad esempio, come dovrebbero allinearsi e connettersi al meglio AWS Config con altri servizi per svolgere il lavoro pesante delle pipeline automatizzate di audit e monitoraggio? I clienti chiedono indicazioni su come ciascun servizio AWS di sicurezza si basa o supporta altri servizi di sicurezza.

Ci occupiamo di ciascuno di questi aspetti nella AWS SRA. La prima priorità nell'elenco (dove vanno le cose) è l'obiettivo del diagramma di architettura principale e delle discussioni che lo accompagnano in questo documento. Forniamo un' AWS Organizations architettura consigliata e una account-by-account descrizione di quali servizi vanno utilizzati. Per iniziare con la seconda priorità dell'elenco

(come pensare all'insieme completo di servizi di sicurezza), leggi la sezione Applica i servizi di sicurezza all'intera AWS organizzazione. Questa sezione descrive un modo per raggruppare i servizi di sicurezza in base alla struttura degli elementi AWS dell'organizzazione. Inoltre, queste stesse idee si riflettono nella discussione sull'account dell'applicazione, che evidenzia come i servizi di sicurezza possono essere gestiti per concentrarsi su determinati livelli dell'account: istanze Amazon Elastic Compute Cloud (Amazon EC2), reti Amazon Virtual Private Cloud (Amazon VPC) e l'account più ampio. Infine, la terza priorità (integrazione dei servizi) si riflette in tutta la guida, in particolare nella discussione dei singoli servizi nelle guide di approfondimento nella libreria AWS SRA e del codice nell'archivio del codice AWS SRA.

Come usare l'SRA AWS

Esistono diversi modi per utilizzare l' AWS SRA a seconda della fase del percorso di adozione del cloud. Ecco un elenco di modi per ottenere il massimo dalle risorse AWS SRA (diagramma di architettura, linee guida scritte ed esempi di codice).

- Definite lo stato di destinazione per la vostra architettura di sicurezza.

  Sia che stiate appena iniziando il vostro Cloud AWS percorso, configurando il primo set di account, sia che stiate pianificando di migliorare un AWS ambiente consolidato, l' AWS SRA è il punto di partenza per costruire la vostra architettura di sicurezza. Iniziate con una base completa di struttura degli account e servizi di sicurezza, quindi adattatela in base al vostro particolare stack tecnologico, alle competenze, agli obiettivi di sicurezza e ai requisiti di conformità. Se sai che dovrai creare e lanciare più carichi di lavoro, puoi prendere la tua versione personalizzata dell' AWS SRA e utilizzarla come base per l'architettura di riferimento per la sicurezza della tua organizzazione. Per scoprire come raggiungere lo stato obiettivo descritto dall' AWS SRA, consulta la sezione Costruire l'architettura di sicurezza: un approccio graduale.
- Rivedi (e rivedi) i progetti e le funzionalità che hai già implementato.

  Se disponete già di una progettazione e di un'implementazione di sicurezza, vale la pena dedicare del tempo a confrontare ciò che avete con l' AWS SRA. L' AWS SRA è progettato per essere completo e fornisce una base diagnostica di base per la revisione della propria sicurezza. Se i vostri progetti di sicurezza sono allineati allo AWS SRA, potete essere più sicuri di seguire le migliori pratiche durante l'utilizzo. Servizi AWS Se i vostri progetti di sicurezza divergono o addirittura non concordano con le linee guida dell' AWS SRA, ciò non è necessariamente un segno che state facendo qualcosa di sbagliato. Invece, questa osservazione vi offre l'opportunità di rivedere il vostro processo decisionale. Esistono motivi aziendali e tecnologici legittimi per

cui potreste discostarvi dalle migliori pratiche AWS SRA. Forse i vostri particolari requisiti di conformità, regolamentazione o sicurezza dell'organizzazione richiedono configurazioni di servizio specifiche. Oppure, anziché utilizzare Servizi AWS, potreste avere una preferenza in termini di funzionalità per un prodotto di AWS Partner Network o per un'applicazione personalizzata da voi creata e gestita. A volte, durante questa revisione, potresti scoprire che le tue decisioni precedenti sono state prese sulla base di tecnologie, AWS funzionalità o vincoli aziendali obsoleti che non si applicano più. Questa è una buona opportunità per rivedere, dare priorità agli aggiornamenti e aggiungerli alla posizione appropriata del backlog tecnico. Qualunque cosa scoprirete valutando la vostra architettura di sicurezza alla luce dell' AWS SRA, troverete utile documentare tale analisi. Avere quel registro storico delle decisioni e delle loro giustificazioni può aiutare a informare e dare priorità alle decisioni future.

- Avvia l'implementazione della tua architettura di sicurezza.

  I moduli AWS SRA infrastructure as code (IaC) forniscono un modo rapido e affidabile per iniziare a creare e implementare l'architettura di sicurezza. Questi moduli sono descritti in modo più approfondito nella sezione relativa all'archivio del codice e nell'archivio pubblico. GitHub Non solo consentono agli ingegneri di basarsi su esempi di alta qualità dei modelli delle linee guida AWS SRA, ma incorporano anche controlli di sicurezza consigliati come le policy sulle password IAM, la crittografia Amazon Simple Storage Service (Amazon S3), l'accesso pubblico agli account di blocco, la crittografia Amazon Elastic Block Store (EC2 Amazon EBS) predefinita di Amazon e l'integrazione AWS Control Tower , in modo che i controlli vengano applicati o rimossi man mano che vengono integrati. o dismesso. Account AWS

- Scopri di più sui servizi e le funzionalità di sicurezza. AWS

  Le linee guida e le discussioni contenute nell' AWS SRA includono caratteristiche importanti e considerazioni sull'implementazione e la gestione per i singoli servizi relativi AWS alla sicurezza e alla protezione. Una caratteristica dell' AWS SRA è che fornisce un'introduzione di alto livello all'ampiezza dei servizi di AWS sicurezza e al modo in cui interagiscono in un ambiente con più account. Ciò integra l'analisi approfondita delle funzionalità e della configurazione di ciascun servizio disponibile in altre fonti. Un esempio di ciò è la discussione su come AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM) acquisisce i risultati di sicurezza da una varietà di Servizi AWS AWS Partner prodotti e persino dalle vostre applicazioni.

- Promuovi una discussione sulla governance organizzativa e sulle responsabilità in materia di sicurezza.

Un elemento importante della progettazione e implementazione di qualsiasi architettura o strategia di sicurezza è capire chi all'interno dell'organizzazione ha quali responsabilità in materia di sicurezza. Ad esempio, la questione di dove aggregare e monitorare i risultati di sicurezza è legata alla questione di quale team sarà responsabile di tale attività. Tutti i risultati dell'organizzazione sono monitorati da un team centrale che deve accedere a un account dedicato agli strumenti di sicurezza? Oppure i singoli team applicativi (o unità aziendali) sono responsabili di determinate attività di monitoraggio e quindi devono accedere a determinati strumenti di avviso e monitoraggio? Come altro esempio, se l'organizzazione ha un gruppo che gestisce tutte le chiavi di crittografia a livello centrale, ciò influirà su chi ha l'autorizzazione a creare AWS Key Management Service (AWS KMS) chiavi e su quali account verranno gestite tali chiavi. Comprendere le caratteristiche della vostra organizzazione, i vari team e le varie responsabilità, vi aiuterà a personalizzare l'SRA per adattarlo al meglio alle vostre esigenze. AWS Al contrario, a volte la discussione sull'architettura di sicurezza diventa lo stimolo per discutere delle responsabilità organizzative esistenti e considerare i potenziali cambiamenti. AWS raccomanda un processo decisionale decentralizzato in cui i team addetti al carico di lavoro siano responsabili della definizione dei controlli di sicurezza in base alle funzioni e ai requisiti dei rispettivi carichi di lavoro. L'obiettivo del team centralizzato di sicurezza e governance è creare un sistema che consenta ai proprietari dei carichi di lavoro di prendere decisioni informate e a tutte le parti di ottenere visibilità sulla configurazione, sui risultati e sugli eventi. L' AWS SRA può essere un veicolo per identificare e informare queste discussioni.

Principali linee guida di implementazione dell'SRA AWS

Ecco otto punti chiave dell' AWS SRA da tenere a mente durante la progettazione e l'implementazione della sicurezza.

- AWS Organizations e un'adeguata strategia multi-account sono elementi necessari della vostra architettura di sicurezza. La corretta separazione di carichi di lavoro, team e funzioni fornisce le basi per la separazione di compiti e strategie. defense-in-depth La guida approfondisce questo aspetto in una sezione successiva.
- Defense-in-depth è una considerazione progettuale importante per la scelta dei controlli di sicurezza per l'organizzazione. Ti aiuta a inserire i controlli di sicurezza appropriati a diversi livelli della AWS Organizations struttura, il che aiuta a ridurre al minimo l'impatto di un problema: se c'è un problema con un livello, sono presenti controlli che isolano altre preziose risorse IT. L' AWS SRA dimostra come Servizi AWS funzioni diverse a diversi livelli dello stack AWS tecnologico e come l'utilizzo combinato di tali servizi contribuisca a raggiungere questi obiettivi. defense-in-depth

Questo defense-in-depth concetto AWS viene ulteriormente discusso in una sezione successiva con esempi di progettazione mostrati in Account dell'applicazione.

- Utilizza l'ampia gamma di elementi costitutivi di sicurezza tra molteplici Servizi AWS funzionalità per creare un'infrastruttura cloud solida e resiliente. Quando personalizzi l' AWS SRA in base alle tue esigenze particolari, considera non solo la funzione Servizi AWS e le caratteristiche principali (ad esempio, autenticazione, crittografia, monitoraggio, politica di autorizzazione), ma anche il modo in cui queste si adattano alla struttura dell'architettura. Una sezione successiva della guida descrive come alcuni servizi funzionano nell'intera AWS organizzazione. Altri servizi funzionano meglio all'interno di un unico account e alcuni sono progettati per concedere o negare l'autorizzazione ai singoli responsabili. Considerare entrambe queste prospettive aiuta a creare un approccio alla sicurezza più flessibile e stratificato.
- Laddove possibile (come descritto nelle sezioni successive), sfruttatene la funzionalità Servizi AWS che può essere implementata in ogni account (distribuita anziché centralizzata) e create un set coerente di barriere condivise che possono aiutare a proteggere i carichi di lavoro da usi impropri e contribuire a ridurre l'impatto degli eventi di sicurezza. L' AWS SRA utilizza AWS Security Hub CSPM (monitoraggio centralizzato dei risultati e controlli di conformità), Amazon GuardDuty (rilevamento delle minacce e rilevamento delle anomalie), AWS Config (monitoraggio delle risorse e rilevamento delle modifiche), IAM Access Analyzer (monitoraggio dell'accesso alle risorse), AWS CloudTrail (registrazione dell'attività delle API del servizio nell'ambiente) e Amazon Macie (classificazione dei dati) come set di base da distribuire su tutti. Servizi AWS Account AWS
- Utilizza la funzionalità di amministrazione delegata di AWS Organizations, laddove è supportata, come spiegato più avanti nella sezione di amministrazione delegata della guida. Ciò consente di registrare un account AWS membro come amministratore per i servizi supportati. L'amministrazione delegata offre ai diversi team dell'azienda la flessibilità necessaria per utilizzare account separati, in base alle rispettive responsabilità, da gestire Servizi AWS in tutto l'ambiente. Inoltre, l'utilizzo di un amministratore delegato consente di limitare l'accesso e gestire il sovraccarico delle autorizzazioni dell'account di gestione. AWS Organizations
- Implementa il monitoraggio, la gestione e la governance centralizzati in tutte le organizzazioni. AWS Utilizzando Servizi AWS questo supporto per l'aggregazione di più account (e talvolta più regioni), insieme alle funzionalità di amministrazione delegata, consentite ai team di progettazione centralizzati di sicurezza, rete e cloud di avere un'ampia visibilità e controllo sulla configurazione di sicurezza e sulla raccolta dei dati appropriate. Inoltre, i dati possono essere restituiti ai team addetti ai carichi di lavoro per consentire loro di prendere decisioni efficaci in materia di sicurezza nelle prime fasi del ciclo di vita dello sviluppo del software (SDLC).

- Utilizzali AWS Control Tower per configurare e gestire il tuo AWS ambiente multi-account con l'implementazione di controlli di sicurezza predefiniti per avviare la build dell'architettura di riferimento per la sicurezza. AWS Control Tower fornisce un modello per fornire gestione delle identità, accesso federato agli account, registrazione centralizzata e flussi di lavoro definiti per il provisioning di account aggiuntivi. È quindi possibile utilizzare la soluzione Customizations for AWS Control Tower (cFCT) per definire come base gli account gestiti AWS Control Tower con controlli di sicurezza, configurazioni di servizio e governance aggiuntivi, come dimostrato dal repository di codici SRA. AWS La funzione account factory fornisce automaticamente ai nuovi account modelli configurabili basati su configurazioni di account approvate per standardizzare gli account all'interno delle organizzazioni. AWS È inoltre possibile estendere la governance a un individuo esistente iscrivendolo a un'unità organizzativa (OU) già governata Account AWS da. AWS Control Tower
- Gli esempi di codice AWS SRA dimostrano come automatizzare l'implementazione dei modelli all'interno della guida AWS SRA utilizzando l'infrastruttura come codice (IaC). Codificando i pattern, è possibile trattare IaC come altre applicazioni dell'organizzazione e automatizzare i test prima di distribuire il codice. IaC aiuta anche a garantire coerenza e ripetibilità implementando guardrail in più ambienti (ad esempio, SDLC o specifici per regione). Gli esempi di codice SRA possono essere implementati in un ambiente multi-account con o senza. AWS Organizations AWS Control Tower Le soluzioni richieste in questo repository AWS Control Tower sono state implementate e testate in un AWS Control Tower ambiente utilizzando AWS CloudFormation and Customizations for (cFCT). AWS Control Tower Le soluzioni che non richiedono AWS Control Tower sono state testate in un AWS Organizations ambiente utilizzando.AWS CloudFormation Se non si utilizza AWS Control Tower, è possibile utilizzare la soluzione di distribuzione AWS Organizations basata.

Nozioni di base sulla sicurezza

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

L' AWS SRA si allinea a tre fondamenti AWS di sicurezza: AWS Cloud Adoption Framework (AWS CAF), AWS Well-Architected e Shared Responsibility Model. AWS

AWS Professional Services ha creato il AWS CAF per aiutare le aziende a progettare e seguire un percorso accelerato verso un'adozione efficace del cloud. Le linee guida e le best practice fornite dal framework ti aiutano a creare un approccio completo al cloud computing in tutta l'azienda e durante l'intero ciclo di vita IT. Il AWS CAF organizza la guida in sei aree di interesse, chiamate prospettive. Ogni prospettiva copre responsabilità distinte possedute o gestite da parti interessate funzionalmente correlate. In generale, le prospettive aziendali, umane e di governance si concentrano sulle capacità aziendali, mentre le prospettive relative alla piattaforma, alla sicurezza e alle operazioni si concentrano sulle capacità tecniche.

La prospettiva di sicurezza del AWS CAF consente di strutturare la selezione e l'implementazione dei controlli in tutta l'azienda. Seguire le attuali AWS raccomandazioni contenute nel pilastro della sicurezza può aiutarvi a soddisfare i requisiti aziendali e normativi.

AWS Well-Architected aiuta gli architetti del cloud a creare un'infrastruttura sicura, ad alte prestazioni, resiliente ed efficiente per le loro applicazioni e carichi di lavoro. Il framework si basa su sei pilastri (eccellenza operativa, sicurezza, affidabilità, efficienza delle prestazioni, ottimizzazione dei costi e sostenibilità) e offre a AWS clienti e partner un approccio coerente per valutare le architetture e implementare progetti scalabili nel tempo. Disporre di carichi di lavoro ben progettati aumenta notevolmente la probabilità di successo aziendale.

Il pilastro di sicurezza Well-Architected Framework descrive come sfruttare le tecnologie cloud per proteggere dati, sistemi e risorse in modo da migliorare il livello di sicurezza. Questo vi aiuterà a soddisfare i requisiti aziendali e normativi seguendo le raccomandazioni attuali. AWS Esistono aree di interesse aggiuntive del Well-Architected Framework che forniscono più contesto per domini specifici come governance, serverless, AI/ML e giochi. Queste sono note come lenti AWS Well-Architected.

La sicurezza e la conformità sono una responsabilità condivisa tra AWS e il cliente. Questo modello condiviso può contribuire ad alleggerire l'onere operativo in quanto AWS opera, gestisce e

controlla i componenti, dal sistema operativo host e dal livello di virtualizzazione fino alla sicurezza fisica delle strutture in cui opera il servizio. Ad esempio, l'utente si assume la responsabilità e la gestione del sistema operativo guest (inclusi gli aggiornamenti e le patch di sicurezza), del software applicativo, della crittografia dei dati sul lato server, delle tabelle delle rotte del traffico di rete e della configurazione del firewall del AWS gruppo di sicurezza fornito. Per i servizi astratti come Amazon S3 e Amazon DynamoDB AWS , gestisce il livello di infrastruttura, il sistema operativo e le piattaforme e accedi agli endpoint per archiviare e recuperare dati. Sei responsabile della gestione dei dati (comprese le opzioni di crittografia), della classificazione degli asset e dell'utilizzo degli strumenti IAM per applicare le autorizzazioni appropriate. Questo modello condiviso viene spesso descritto dicendo che AWS sei responsabile della sicurezza del cloud (ovvero della protezione dell'infrastruttura che gestisce tutti i servizi offerti Cloud AWS) e che tu sei responsabile della sicurezza nel cloud (in base Cloud AWS ai servizi che scegli).

Nell'ambito delle linee guida fornite da questi documenti fondamentali, due serie di concetti sono particolarmente importanti per la progettazione e la comprensione dell' AWS SRA: le funzionalità di sicurezza e i principi di progettazione della sicurezza.

Funzionalità di sicurezza

La prospettiva di sicurezza del AWS CAF delinea nove funzionalità che aiutano a raggiungere la riservatezza, l'integrità e la disponibilità dei dati e dei carichi di lavoro cloud.

- Governance della sicurezza per sviluppare e comunicare ruoli, responsabilità, politiche, processi e procedure di sicurezza nell'ambiente dell'organizzazione. AWS
- Garanzia di sicurezza per monitorare, valutare, gestire e migliorare l'efficacia dei programmi di sicurezza e privacy.
- Gestione delle identità e degli accessi per gestire identità e autorizzazioni su larga scala.
- Rilevamento delle minacce per comprendere e identificare potenziali configurazioni errate di sicurezza, minacce o comportamenti imprevisti.
- Gestione delle vulnerabilità per identificare, classificare, correggere e mitigare continuamente le vulnerabilità di sicurezza.
- Protezione dell'infrastruttura per convalidare la protezione dei sistemi e dei servizi all'interno dei carichi di lavoro.
- Protezione dei dati per mantenere la visibilità e il controllo sui dati e su come accedervi e utilizzarli nell'organizzazione.

- Sicurezza delle applicazioni per aiutare a rilevare e risolvere le vulnerabilità di sicurezza durante il processo di sviluppo del software.
- Risposta agli incidenti per ridurre i potenziali danni rispondendo efficacemente agli incidenti di sicurezza.

Principi di progettazione della sicurezza

Il pilastro della sicurezza di Well-Architected Framework racchiude una serie di sette principi di progettazione che trasformano aree di sicurezza specifiche in linee guida pratiche che possono aiutarti a rafforzare la sicurezza del carico di lavoro. Laddove le funzionalità di sicurezza fanno da cornice alla strategia di sicurezza generale, questi principi del Well-Architected Framework descrivono cosa si può iniziare a fare. Si riflettono in modo molto preciso in questo AWS SRA e consistono nei seguenti elementi:

- Implementate una solida base di identità – Implementate il principio del privilegio minimo e applicate la separazione dei compiti con l'autorizzazione appropriata per ogni interazione con le vostre risorse. AWS Centralizza la gestione delle identità e mira a eliminare la dipendenza dalle credenziali statiche a lungo termine.
- Abilita la tracciabilità – Monitora, genera avvisi e verifica le azioni e le modifiche all'ambiente in tempo reale. Integra la raccolta di log e parametri con i sistemi per analizzare e intervenire automaticamente.
- Applica la sicurezza a tutti i livelli – Applica un defense-in-depth approccio con più controlli di sicurezza. Applica diversi tipi di controlli (ad esempio controlli preventivi e di rilevamento) a tutti i livelli, tra cui edge of network, cloud privato virtuale (VPC), bilanciamento del carico, servizi di istanza e calcolo, sistema operativo, configurazione delle applicazioni e codice.
- Automatizza le best practice di sicurezza – I meccanismi di sicurezza automatizzati e basati su software migliorano la capacità di scalare in modo sicuro, più rapido ed economico. Crea architetture sicure e implementa controlli definiti e gestiti come codice in modelli con controllo di versione.
- Proteggi i dati in transito e a riposo – Classizza i dati in base a livelli di sensibilità e utilizza meccanismi come la crittografia, la tokenizzazione e il controllo degli accessi, ove appropriato.
- Tieni le persone lontane dai dati – Utilizza meccanismi e strumenti per ridurre o eliminare la necessità di accedere direttamente o elaborare manualmente i dati. Ciò riduce il rischio di perdita, modifica e altri errori umani durante la gestione dei dati sensibili.

- Preparati agli eventi di sicurezza – Preparati a un incidente adottando politiche e processi di gestione degli incidenti e indagini in linea con i requisiti organizzativi. Esegui simulazioni di risposta agli incidenti e utilizza strumenti dotati di automazione per aumentare la velocità nel rilevamento, nell'indagine e nel ripristino.

Come utilizzare l' AWS SRA con AWS CAF e Well-Architected Framework AWS

AWS CAF, AWS Well-Architected Framework AWS e SRA sono framework complementari che collaborano per supportare le attività di migrazione e modernizzazione del cloud.

- Il AWS CAF sfrutta l' AWS esperienza e le migliori pratiche per aiutarvi ad allineare i valori dell'adozione del cloud ai risultati aziendali desiderati. Utilizzate il AWS CAF per identificare e dare priorità alle opportunità di trasformazione, valutare e migliorare la predisposizione al cloud e far evolvere iterativamente la vostra roadmap di trasformazione.
- Il AWS Well-Architected Framework AWS fornisce consigli per creare un'infrastruttura sicura, ad alte prestazioni, resiliente ed efficiente per una varietà di applicazioni e carichi di lavoro in grado di soddisfare i risultati aziendali.
- L'AWS SRA aiuta a capire come implementare e gestire i servizi di sicurezza in un modo in linea con le raccomandazioni del AWS CAF e del Well-Architected Framework. AWS

Ad esempio, la prospettiva della sicurezza del AWS CAF suggerisce di valutare come gestire centralmente le identità della forza lavoro e la loro autenticazione. AWS Sulla base di queste informazioni, potresti decidere di utilizzare una soluzione di provider di identità aziendale (IdP) nuova o esistente come Okta, Active Directory o Ping Identity per questo scopo. Segui le indicazioni del AWS Well-Architected Framework e decidi di integrare il tuo IdP con AWS IAM Identity Center il per offrire ai tuoi dipendenti un'esperienza di single sign-on in grado di sincronizzare le appartenenze e le autorizzazioni ai gruppi. Leggi la raccomandazione AWS SRA di abilitare IAM Identity Center nell'account di gestione della tua AWS organizzazione e di amministrarlo tramite un account di strumenti di sicurezza utilizzato dal tuo team addetto alle operazioni di sicurezza. Questo esempio illustra come il AWS CAF aiuta a prendere le decisioni iniziali sul livello di sicurezza desiderato, il AWS Well-Architected Framework fornisce le indicazioni su come valutare le risorse disponibili per raggiungere Servizi AWS tale obiettivo e l' AWS SRA fornisce quindi consigli su come implementare e gestire i servizi di sicurezza selezionati.

Elementi costitutivi della SRA: AWS Organizations conti e barriere

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

AWS I servizi di sicurezza, i relativi controlli e le interazioni vengono utilizzati al meglio sulla base di una strategia AWS multi-account e di barriere di gestione delle identità e degli accessi. Queste barriere consentono di implementare i privilegi minimi, la separazione dei compiti e la privacy e forniscono supporto per le decisioni sui tipi di controlli necessari, su dove viene gestito ciascun servizio di sicurezza e su come condividere dati e autorizzazioni nell'SRA. AWS

An Account AWS fornisce limiti di sicurezza, accesso e fatturazione per le risorse e consente di raggiungere l' AWS indipendenza e l'isolamento delle risorse. L'uso di più account Account AWS svolge un ruolo importante nel modo in cui si soddisfano i requisiti di sicurezza, come illustrato nella Account AWS sezione Vantaggi dell'utilizzo di più account del white paper Organizzare AWS l'ambiente utilizzando più account. Ad esempio, è possibile organizzare i carichi di lavoro in account separati e account di gruppo all'interno di un'unità organizzativa (OU) in base alla funzione, ai requisiti di conformità o a un insieme comune di controlli anziché rispecchiare la struttura di reporting dell'azienda. Tieni a mente la sicurezza e l'infrastruttura per consentire all'azienda di stabilire barriere comuni man mano che i carichi di lavoro crescono. Questo approccio offre confini e controlli solidi tra i carichi di lavoro. La separazione a livello di account, in combinazione con AWS Organizations, viene utilizzata per isolare gli ambienti di produzione dagli ambienti di sviluppo e test o per fornire un forte confine logico tra i carichi di lavoro che elaborano dati di diverse classificazioni come Payment Card Industry Data Security Standard (PCI DSS) o Health Insurance Portability and Accountability Act (HIPAA). Sebbene tu possa iniziare il tuo AWS percorso con un solo account, ti AWS consiglia di configurare più account man mano che i carichi di lavoro aumentano in dimensioni e complessità.

Le autorizzazioni consentono di specificare l'accesso alle risorse. AWS Le autorizzazioni vengono concesse alle entità IAM note come responsabili (utenti, gruppi e ruoli). Per impostazione predefinita, i principali iniziano senza autorizzazioni. I responsabili IAM non possono fare nulla AWS finché non concedi loro le autorizzazioni e puoi impostare barriere che si applichino tanto ampiamente quanto l'intera AWS organizzazione o che siano granulari come una combinazione individuale di principi, azioni, risorse e condizioni.

Utilizzo per motivi di sicurezza AWS Organizations

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

AWS Organizationsti aiuta a gestire e governare centralmente il tuo ambiente man mano che cresci e scalerai le tue AWS risorse. In questo modo AWS Organizations, puoi crearne di nuovi Account AWS, allocare risorse, raggruppare account per organizzare i carichi di lavoro in modo programmatico e applicare politiche ad account o gruppi di account per la governance. Un' AWS organizzazione consolida i tuoi dati Account AWS in modo da poterli amministrare come un'unica unità. Ha un account di gestione oltre a zero o più account membri. La maggior parte dei carichi di lavoro risiede negli account dei membri, ad eccezione di alcuni processi gestiti centralmente che devono risiedere nell'account di gestione o negli account assegnati come amministratori delegati, in alcuni casi. Servizi AWS Puoi fornire strumenti e accesso da una posizione centrale al tuo team di sicurezza per gestire le esigenze di sicurezza per conto di un'organizzazione. AWS È possibile ridurre la duplicazione delle risorse condividendo le risorse critiche all'interno AWS dell'organizzazione. Puoi raggruppare gli account in unità AWS organizzative (OUs), che possono rappresentare ambienti diversi in base ai requisiti e allo scopo del carico di lavoro. AWS Organizations fornisce inoltre diverse politiche che consentono di applicare centralmente controlli di sicurezza aggiuntivi a tutti gli account membri delle organizzazioni. Questa sezione si concentra sulle politiche di controllo dei servizi (SCPs), sulle politiche di controllo delle risorse (RCPs) e sulle politiche dichiarative.

Con AWS Organizations, è possibile utilizzare SCPse RCPsapplicare barriere di autorizzazione a livello di AWS organizzazione, unità organizzativa o account. SCPs sono barriere che si applicano ai responsabili all'interno dell'account di un'organizzazione, ad eccezione dell'account di gestione (che è uno dei motivi per non eseguire carichi di lavoro in questo account). Quando si collega un SCP a un'unità organizzativa, l'SCP viene ereditato dal figlio e dagli account relativi a tale unità organizzativa. OUs SCPs non concedete alcuna autorizzazione. Al contrario, specificano le autorizzazioni massime disponibili per i responsabili di un' AWS organizzazione, un'unità organizzativa o un account. È comunque necessario allegare politiche basate sull'identità o sulle risorse ai responsabili o alle risorse dell'azienda per concedere loro effettivamente le autorizzazioni. Account AWS Ad esempio, se un SCP nega l'accesso a tutto Amazon S3, un principale interessato dall'SCP non avrà accesso ad Amazon S3 anche se gli viene esplicitamente concesso l'accesso tramite una policy IAM. Per ulteriori informazioni su come vengono valutate le politiche IAM, sul ruolo

e su come l'accesso viene infine concesso o negato SCPs, consulta Logica di valutazione delle politiche nella documentazione IAM.

RCPs sono barriere che si applicano alle risorse all'interno degli account di un'organizzazione, indipendentemente dal fatto che le risorse appartengano alla stessa organizzazione. Ad esempio SCPs, RCPs non influiscono sulle risorse dell'account di gestione e non concedono alcuna autorizzazione. Quando si collega un RCP a un'unità organizzativa, l'RCP viene ereditato dal figlio OUs e dagli account dell'unità organizzativa. RCPs forniscono il controllo centralizzato sulle autorizzazioni massime disponibili per le risorse dell'organizzazione e attualmente supportano un sottoinsieme di. Servizi AWS Quando progetti SCPs per te OUs, ti consigliamo di valutare le modifiche utilizzando il simulatore di policy IAM. Dovresti anche esaminare l'ultimo accesso ai dati del servizio in IAM e utilizzarli AWS CloudTrail per registrare l'utilizzo del servizio a livello di API per comprendere il potenziale impatto delle modifiche SCP.

SCPs e RCPs sono controlli indipendenti. Puoi scegliere di abilitare solo SCPs o RCPs utilizzare entrambi i tipi di policy insieme in base ai controlli di accesso che desideri applicare. Ad esempio, se si desidera impedire ai responsabili dell'organizzazione di accedere a risorse esterne all'organizzazione, è possibile applicare questo controllo utilizzando. SCPs Se desideri limitare o impedire alle identità esterne di accedere alle tue risorse, applichi questo controllo utilizzando. RCPs Per ulteriori informazioni e casi d'uso per RCPs e SCPs, consulta Using SCPs and RCPs nella AWS Organizations documentazione.

È possibile utilizzare le politiche AWS Organizations dichiarative per dichiarare e applicare centralmente la configurazione desiderata per un determinato aspetto su larga scala Servizio AWS all'interno dell'organizzazione. Ad esempio, puoi bloccare l'accesso pubblico a Internet alle risorse Amazon VPC in tutta l'organizzazione. A differenza delle politiche di autorizzazione come SCPs e RCPs, le politiche dichiarative vengono applicate nel piano di controllo di un AWS servizio. Le politiche di autorizzazione regolano l'accesso APIs, mentre le politiche dichiarative vengono applicate direttamente a livello di servizio per imporre un intento duraturo. Queste politiche aiutano a garantire che la configurazione di base di an Servizio AWS venga sempre mantenuta, anche quando il servizio introduce nuove funzionalità o. APIs La configurazione di base viene mantenuta anche quando vengono aggiunti nuovi account a un'organizzazione o quando vengono creati nuovi responsabili e risorse. Le politiche dichiarative possono essere applicate a un'intera organizzazione o a specifici OUs account.

Ognuno Account AWS ha un singolo utente root che dispone di autorizzazioni complete per tutte le AWS risorse per impostazione predefinita. Come best practice di sicurezza, si consiglia di non utilizzare l'utente root ad eccezione di alcune attività che richiedono esplicitamente un utente root.

Se gestisci più account Account AWS AWS Organizations, puoi disabilitare centralmente l'accesso root e quindi eseguire azioni con privilegi root per conto di tutti gli account membri. Dopo aver gestito centralmente l'accesso root per gli account dei membri, puoi eliminare la password dell'utente root, le chiavi di accesso e i certificati di firma e disattivare l'autenticazione a più fattori (MFA) per gli account membro. Per impostazione predefinita, i nuovi account creati con accesso root gestito centralmente non hanno credenziali utente root. Gli account dei membri non possono accedere con il proprio utente root o eseguire il recupero della password per il proprio utente root.

AWS Control Toweroffre un modo semplificato per configurare e gestire più account. Automatizza la configurazione degli account nell' AWS organizzazione, automatizza il provisioning, applica i controlli (che includono controlli preventivi e investigativi) e fornisce una dashboard per la visibilità. Un'ulteriore policy di gestione IAM, un limite di autorizzazioni, è associata a specifici principali IAM (utenti o ruoli) e imposta le autorizzazioni massime che una policy basata sull'identità può concedere a un responsabile IAM.

AWS Organizations ti aiuta a configurare Servizi AWSin modo che si applichino a tutti i tuoi account. Ad esempio, puoi configurare la registrazione centralizzata di tutte le azioni eseguite all'interno AWS dell'organizzazione utilizzando CloudTrail e impedire agli account dei membri di disabilitare la registrazione. Puoi anche aggregare centralmente i dati per le regole che hai definito utilizzando AWS Config, in modo da verificare la conformità dei carichi di lavoro e reagire rapidamente alle modifiche. Puoi utilizzarli AWS CloudFormation StackSetsper gestire centralmente gli CloudFormation stack tra gli account e all'interno AWS dell'organizzazione, OUs in modo da poter fornire automaticamente un nuovo account per soddisfare i tuoi requisiti di sicurezza.

La configurazione predefinita prevede l' AWS Organizations utilizzo SCPs come liste di rifiuto. Utilizzando una strategia di elenco di utenti non autorizzati, gli amministratori degli account membri possono delegare tutti i servizi e le azioni fino a quando non si crea e si allega un SCP che neghi un servizio o una serie di azioni specifici. Le dichiarazioni di rifiuto richiedono meno manutenzione rispetto a un elenco consentito, perché non è necessario aggiornarle quando si aggiungono nuovi servizi. AWS Le istruzioni Deny sono generalmente più corte nella lunghezza dei caratteri, quindi è più facile rispettare la dimensione massima per. SCPs In un'istruzione in cui l'`Effect`elemento ha un valore di`Deny`, è inoltre possibile limitare l'accesso a risorse specifiche o definire le condizioni relative all'entrata SCPs in vigore. Al contrario, un'`Allow`istruzione in un SCP si applica a tutte le risorse (`"*"`) e non può essere limitata da condizioni. Per ulteriori informazioni ed esempi, vedete Strategie per l'utilizzo SCPs nella AWS Organizations documentazione.

Considerazioni di natura progettuale

- In alternativa, per utilizzarlo SCPs come elenco consentito, devi sostituire l'`FullAWSAccess`SCP gestito da AWS con un SCP che consenta esplicitamente solo i servizi e le azioni che desideri consentire. Affinché un'autorizzazione sia abilitata per un account specifico, ogni SCP (dalla radice a ciascuna unità organizzativa nel percorso diretto verso l'account e persino collegato all'account stesso) deve consentire tale autorizzazione. Questo modello è di natura più restrittiva e potrebbe essere adatto a carichi di lavoro altamente regolamentati e sensibili. Questo approccio richiede l'autorizzazione esplicita di ogni servizio o azione IAM nel percorso dall'unità organizzativa all'unità organizzativa Account AWS .
- Idealmente, si utilizzerebbe una combinazione di strategie di elenco di rifiuto e di elenco consentito. Utilizzate l'elenco delle autorizzazioni consentite per definire l'elenco delle autorizzazioni Servizi AWS approvate da utilizzare all'interno di un' AWS organizzazione e allegate questo SCP alla radice dell'organizzazione AWS . Se disponi di un set diverso di servizi consentiti per il tuo ambiente di sviluppo, collegherai il rispettivo SCPs a ciascuna unità organizzativa. È quindi possibile utilizzare l'elenco di negazione per definire i guardrail aziendali negando esplicitamente azioni IAM specifiche.
- RCPs si applicano alle risorse per un sottoinsieme di. Servizi AWS Per ulteriori informazioni, consulta Elenco di Servizi AWS tale supporto RCPs nella AWS Organizations documentazione. La configurazione predefinita dei AWS Organizations supporti utilizzati RCPs come elenchi di negazione. Quando viene attivata RCPs nell'organizzazione, una policy AWS gestita richiamata `RCPFullAWSAccess` viene automaticamente allegata alla radice dell'organizzazione, a ogni unità organizzativa e a ogni account dell'organizzazione. Non è possibile scollegare questa politica. Questo RCP predefinito consente l'accesso a tutti i principali e alle azioni tramite la valutazione RCP. Ciò significa che fino a quando non inizi a creare e allegare RCPs, tutte le autorizzazioni IAM esistenti continueranno a funzionare come prima. Questa policy AWS gestita non concede l'accesso. È quindi possibile creare un nuovo RCPs elenco di dichiarazioni di rifiuto per bloccare l'accesso alle risorse dell'organizzazione.

L'account di gestione, l'accesso affidabile e gli amministratori delegati

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

L'account di gestione (chiamato anche account di gestione dell' AWS organizzazione o account di gestione dell'organizzazione) è unico e diverso da tutti gli altri account. AWS OrganizationsÈ l'account che crea l' AWS organizzazione. Da questo account è possibile creare all' AWS interno dell'organizzazione, invitare altri account esistenti Account AWS nell' AWS organizzazione (entrambi i tipi sono considerati account membro), rimuovere account dall' AWS organizzazione e applicare le politiche IAM alla radice o agli account all'interno dell' AWS organizzazione. OUs

L'account di gestione implementa protezioni di sicurezza universali tramite SCPs implementazioni di servizi (ad esempio CloudTrail) che influiranno su tutti gli account dei membri dell'organizzazione. RCPs AWS Per limitare ulteriormente le autorizzazioni nell'account di gestione, tali autorizzazioni possono essere delegate a un altro account appropriato, ad esempio un account di sicurezza, ove possibile.

L'account di gestione ha le responsabilità di un account di pagamento ed è responsabile del pagamento di tutte le spese sostenute dagli account membri. Non è possibile cambiare l'account di gestione di un' AWS organizzazione. An Account AWS può essere membro di una sola AWS organizzazione alla volta.

A causa della funzionalità e dell'ambito di influenza dell'account di gestione, si consiglia di limitare l'accesso a questo account e di concedere le autorizzazioni solo ai ruoli che le richiedono. Due funzionalità che consentono di eseguire questa operazione sono l'accesso affidabile e l'amministratore delegato. È possibile utilizzare l'accesso affidabile per consentire a un Servizio AWS utente specificato, denominato servizio affidabile, di eseguire attività nell' AWS organizzazione e nei relativi account per conto dell'utente. Ciò comporta la concessione di autorizzazioni per il servizio attendibile, ma in caso contrario non influenza le autorizzazioni per i ruoli o gli utenti IAM. È possibile utilizzare l'accesso affidabile per specificare le impostazioni e i dettagli di configurazione che si desidera che il servizio affidabile mantenga negli account AWS dell'organizzazione per conto dell'utente. Ad esempio, la sezione relativa agli account di gestione dell'organizzazione dell' AWS SRA spiega come concedere al CloudTrail servizio un accesso affidabile per creare un percorso CloudTrail organizzativo in tutti gli account AWS dell'organizzazione.

Alcuni Servizi AWS supportano la funzionalità di amministratore delegato in. AWS Organizations Con questa funzionalità, i servizi compatibili possono registrare un account AWS membro nell' AWS organizzazione come amministratore degli account dell' AWS organizzazione in quel servizio. Questa funzionalità offre ai diversi team dell'azienda la flessibilità necessaria per utilizzare account separati, in base alle rispettive responsabilità, da gestire Servizi AWS in tutto l'ambiente. I servizi AWS di sicurezza dell' AWS SRA che attualmente supportano l'amministratore delegato includono IAM Identity Center,, AWS Firewall Manager Amazon AWS Config, IAM Access Analyzer GuardDuty, Amazon Macie, AWS Security Hub Cloud Security Posture Management (), Amazon Detective,AWS Security Hub CSPM Amazon AWS Audit Manager Inspector e. AWS Systems Manager L'uso della funzionalità di amministratore delegato è enfatizzato nell' AWS SRA come best practice e deleghiamo l'amministrazione dei servizi relativi alla sicurezza all'account Security Tooling.

Struttura degli account dedicata

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

An Account AWS fornisce sicurezza, accesso e limiti di fatturazione per le AWS risorse e consente di raggiungere l'indipendenza e l'isolamento delle risorse. Per impostazione predefinita, non è consentito l'accesso tra account.

Quando progetti l'unità organizzativa e la struttura degli account, inizia pensando alla sicurezza e all'infrastruttura. Ti consigliamo di creare un set di funzionalità di base OUs per queste funzioni specifiche, suddivise in Infrastruttura e Sicurezza OUs. Questi consigli sulle unità organizzative e sugli account racchiudono un sottoinsieme delle nostre linee guida più ampie AWS Organizations e complete per la progettazione di strutture multi-account. Per una serie completa di consigli, consulta Organization your AWS environment using multiple account nella AWS documentazione e il post di blog Best practice for organizational units with. AWS Organizations

L' AWS SRA utilizza i seguenti account per eseguire operazioni di sicurezza efficaci su. AWS Questi account dedicati aiutano a garantire la separazione delle mansioni, supportano diverse politiche di governance e accesso per diversi aspetti sensibili di applicazioni e dati e aiutano a mitigare l'impatto di un evento di sicurezza. Nelle discussioni che seguono, ci concentriamo sugli account di produzione (di produzione) e sui carichi di lavoro associati. Gli account SDLC (Software Development Lifecycle) (spesso denominati account di sviluppo e test) sono destinati alla gestione temporanea dei risultati

finali e possono funzionare secondo una serie di politiche di sicurezza diverse da quelle degli account di produzione.

Account	OU	Ruolo di sicurezza
Gestione	—	Governance e gestione centralizzate di tutti Regioni AWS e degli account. Il Account AWS che ospita la radice dell' AWS organ izzazione.
Strumenti di sicurezza	Sicurezza	Dedicato alla Account AWS gestione di servizi di sicurezza di ampia portata (come Security Hub CSPM GuardDuty, Audit Manager, Detective, Amazon Inspector e AWS Config), al monitoraggio e all'automazione degli avvisi e delle Account AWS risposte di sicurezza. (In AWS Control Tower, il nome predefinito dell'account in Security OU è Audit account.)
Archivio dei registri	Sicurezza	Dedicato Account AWS all'acquisizione e all'archi viazione di tutti i log e i backup per tutti e. Regioni AWS Account AWS Questo dovrebbe essere progettato come storage immutabile.
Rete	Infrastruttura	Il gateway tra l'applicazione e la rete Internet più ampia. L'account di rete isola i servizi

		di rete, la configurazione e il funzionamento più ampi dai carichi di lavoro, dalla sicurezza e da altre infrastru tture delle singole applicazioni.
Servizi condivisi	Infrastruttura	Questo account supporta i servizi utilizzati da più applicazioni e team per fornire i propri risultati. Gli esempi includono i servizi di directory di Identity Center (Active Directory), i servizi di messaggistica e i servizi di metadati.
Applicazione	Carichi di lavoro	Account AWS che ospitano le applicazioni AWS dell'orga nizzazione ed eseguono i carichi di lavoro. (A volte vengono chiamati account Workload). Gli account delle applicazioni devono essere creati per isolare i servizi software anziché essere mappati ai team. Ciò rende l'applicazione distribuita più resistente ai cambiamenti organizzativi.

AWS struttura organizzativa e contabile dell'SRA AWS

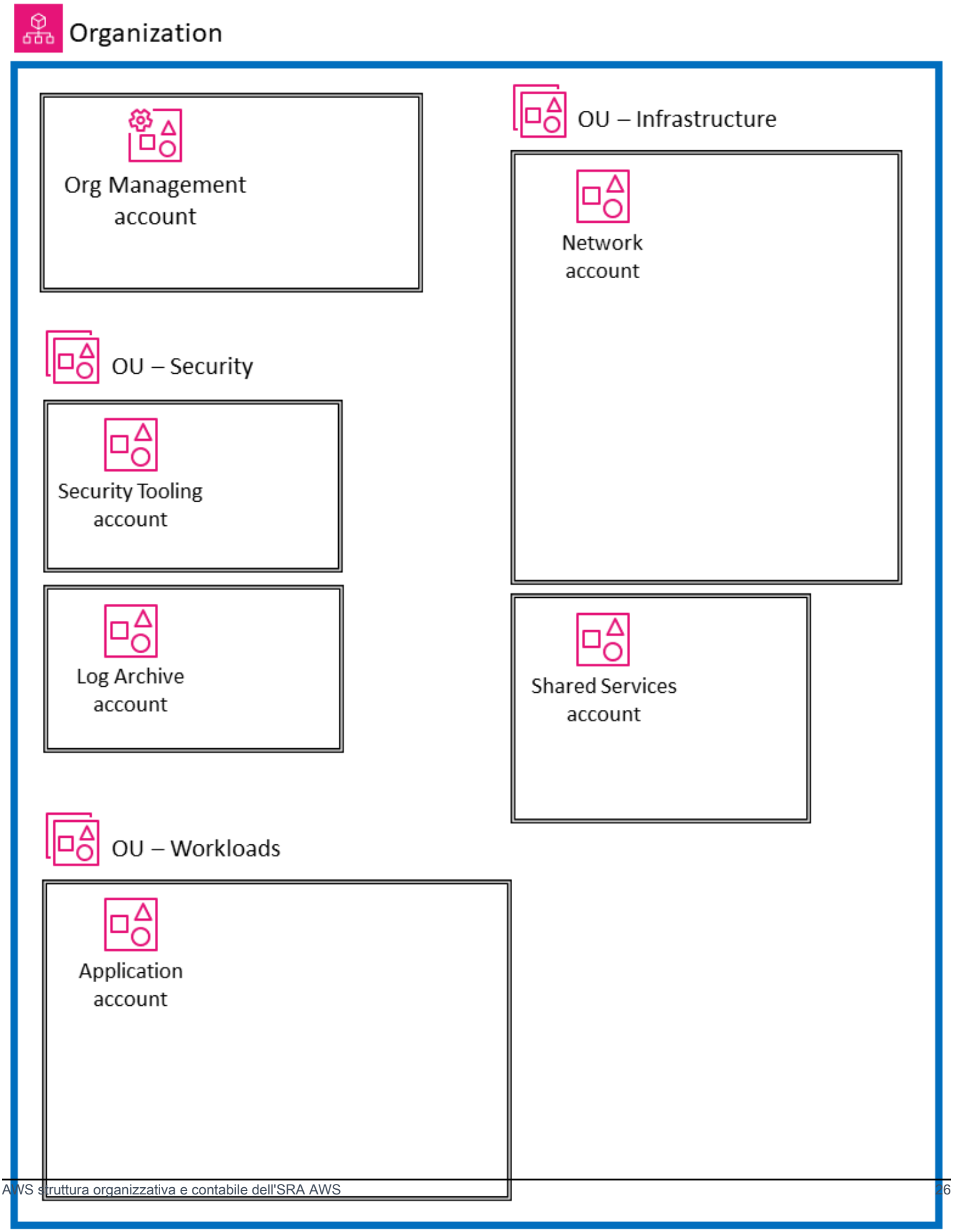
Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

Il diagramma seguente illustra la struttura di alto livello dell' AWS SRA senza visualizzare servizi specifici. Riflette la struttura degli account dedicati discussa nella sezione precedente e includiamo il diagramma qui per orientare la discussione sui componenti principali dell'architettura:

- Tutti gli account mostrati nel diagramma fanno parte di un'unica organizzazione. AWS
- Nella parte superiore sinistra del diagramma c'è l'account di gestione dell'organizzazione, utilizzato per creare l' AWS organizzazione.
- Sotto l'account Org Management si trova l'unità organizzativa di sicurezza con due account specifici: uno per Security Tooling e l'altro per Log Archive.
- Sul lato destro si trova l'unità organizzativa dell'infrastruttura con l'account di rete e l'account Shared Services.
- Nella parte inferiore del diagramma c'è l'unità organizzativa Workloads, associata a un account dell'applicazione che ospita l'applicazione aziendale.

Ai fini di questa guida, tutti gli account sono considerati account di produzione (produzione) che operano in un unico account. Regione AWS La maggior parte Servizi AWS (ad eccezione dei servizi globali) ha un ambito regionale, il che significa che i piani di controllo e dati del servizio esistono indipendentemente in ciascuno di essi. Regione AWS Per questo motivo, è necessario replicare questa architettura su tutto ciò Regioni AWS che si prevede di utilizzare, per garantire la copertura dell'intero ambiente. AWS Se non disponi di carichi di lavoro in una regione specifica Regione AWS, devi disabilitare la regione utilizzando SCPso utilizzando meccanismi di registrazione e monitoraggio. È possibile utilizzare Security Hub CSPM per aggregare risultati e punteggi di sicurezza da più aree di aggregazione Regioni AWS a una singola regione di aggregazione per una visibilità centralizzata.

Quando si ospita un' AWS organizzazione con un ampio set di account, è utile disporre di un livello di orchestrazione che faciliti l'implementazione e la governance degli account. AWS Control Tower offre un modo semplice per configurare e gestire un ambiente con più account. AWS Gli esempi di codice AWS SRA presenti nel GitHub repository dimostrano come utilizzare la soluzione Customizations for AWS Control Tower (cFCT) per implementare le strutture consigliate da SRA. AWS

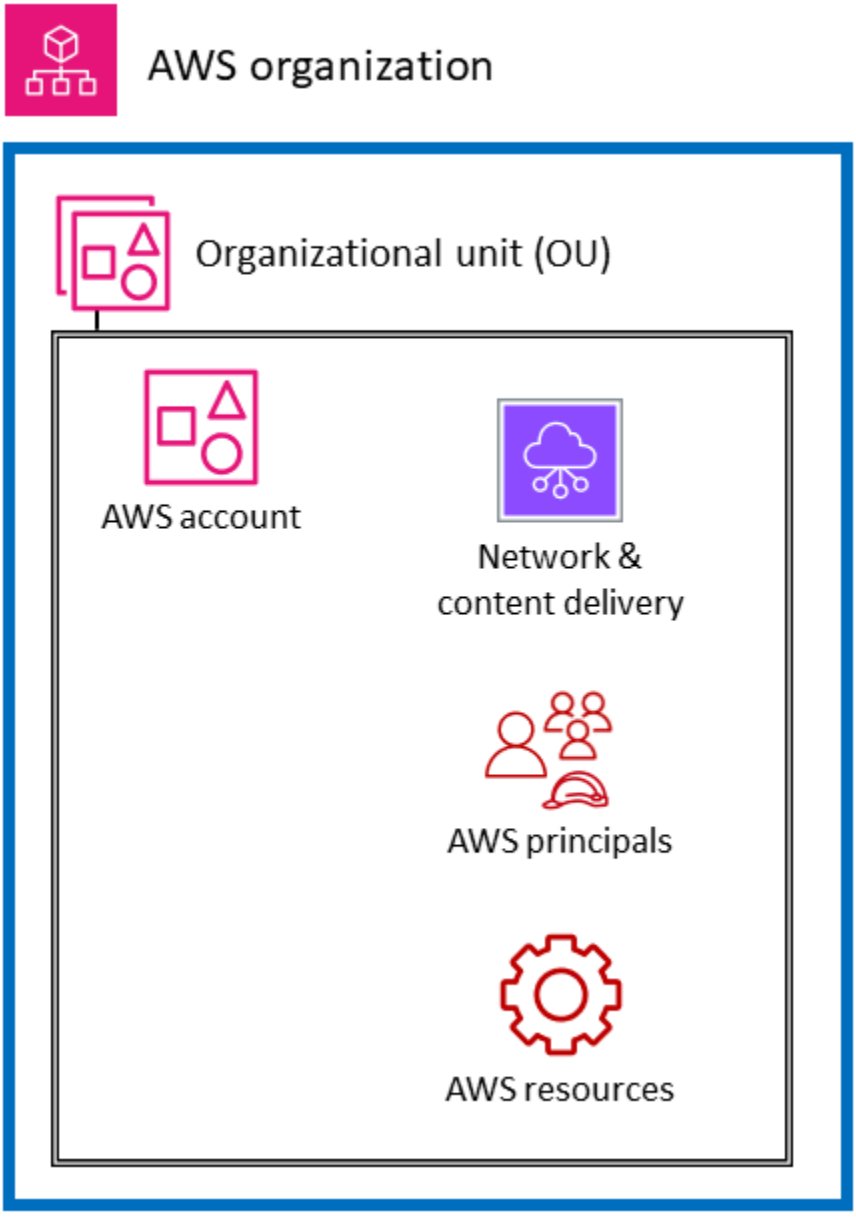

Organization
Org Management account
OU – Infrastructure
Network account
OU – Security
Security Tooling account
Log Archive account
Shared Services account
OU – Workloads
Application account

Applica i servizi di sicurezza in tutta l'organizzazione AWS

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

Come descritto in una sezione precedente, i clienti sono alla ricerca di un altro modo per pensare e organizzare strategicamente l'intera gamma di servizi di AWS sicurezza. L'approccio organizzativo più comune oggi consiste nel raggruppare i servizi di sicurezza per funzione principale, in base alle funzioni di ciascun servizio. La prospettiva di sicurezza del AWS CAF elenca nove funzionalità funzionali, tra cui la gestione delle identità e degli accessi, la protezione dell'infrastruttura, la protezione dei dati e il rilevamento delle minacce. L' Servizi AWS abbinamento a queste capacità funzionali è un modo pratico per prendere decisioni di implementazione in ogni area. Ad esempio, per quanto riguarda la gestione delle identità e degli accessi, IAM e IAM Identity Center sono servizi da prendere in considerazione. Quando si progetta l'approccio al rilevamento delle minacce, GuardDuty potrebbe essere la prima considerazione da prendere in considerazione.

Oltre a questa visione funzionale, puoi anche visualizzare la tua sicurezza con una visione strutturale trasversale. Cioè, oltre a chiedere: «Cosa Servizi AWS devo usare per controllare e proteggere le mie identità, l'accesso logico o i meccanismi di rilevamento delle minacce?» , puoi anche chiedere: «Cosa Servizi AWS devo applicare a tutta la mia AWS organizzazione? Quali sono i livelli di difesa che devo mettere in atto per proteggere le istanze Amazon EC2 alla base della mia applicazione?» In questa visualizzazione, esegui la Servizi AWS mappatura delle funzionalità ai livelli del tuo AWS ambiente. Alcuni servizi e funzionalità si adattano perfettamente all'implementazione dei controlli nell'intera AWS organizzazione. Ad esempio, il blocco dell'accesso pubblico ai bucket Amazon S3 è un controllo specifico a questo livello. Dovrebbe essere preferibilmente eseguito presso l'organizzazione principale anziché far parte della configurazione dell'account individuale. Altri servizi e funzionalità sono utilizzati al meglio per proteggere le singole risorse all'interno di un Account AWS. L'implementazione di un'autorità di certificazione (CA) subordinata all'interno di un account che richiede certificati TLS privati è un esempio di questa categoria. Un altro raggruppamento altrettanto importante è costituito dai servizi che hanno un effetto sul livello di rete virtuale dell'infrastruttura. AWS Il diagramma seguente mostra sei livelli in un AWS ambiente tipico: AWS organizzazione, unità organizzativa (OU), account, infrastruttura di rete, principali e risorse.



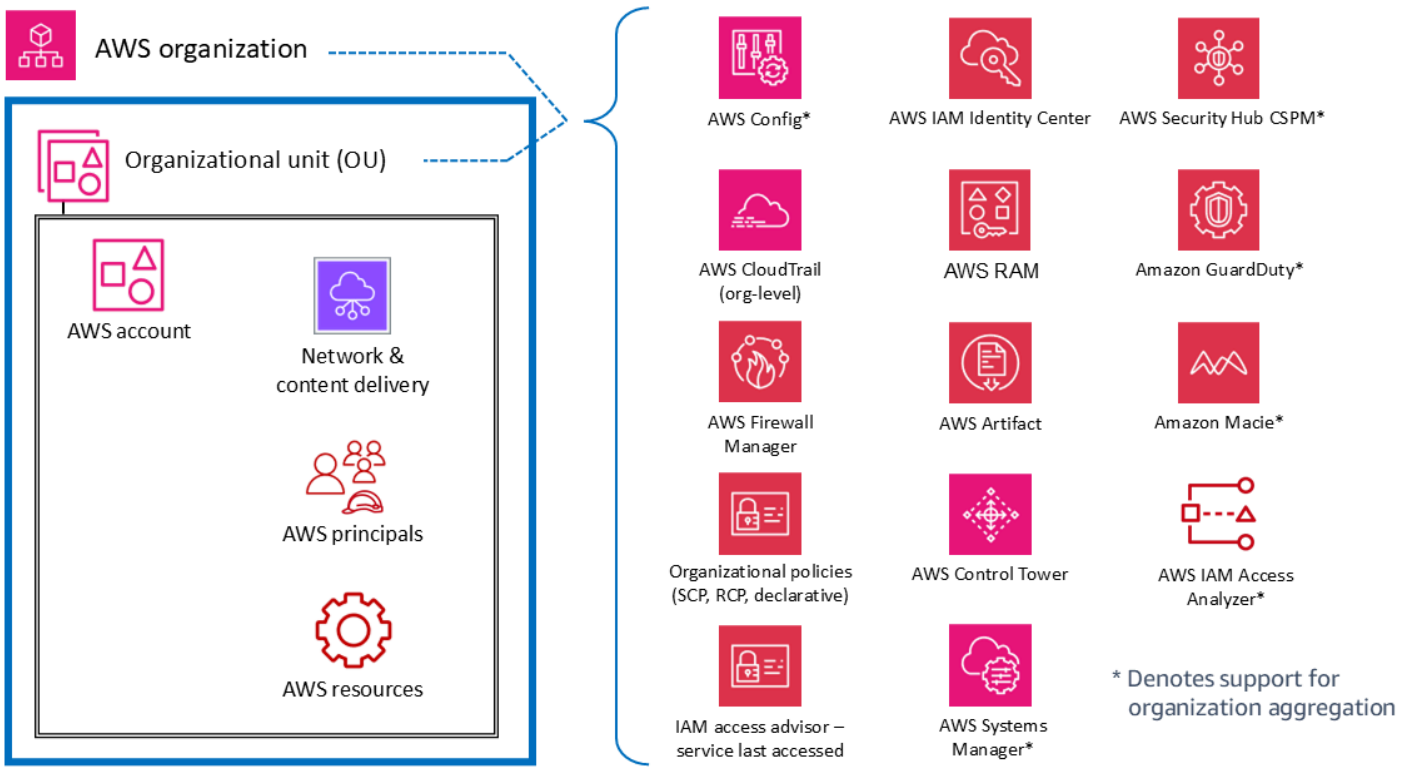
La comprensione dei servizi in questo contesto strutturale, compresi i controlli e le protezioni a ogni livello, aiuta a pianificare e implementare una defense-in-depth strategia in tutto l' AWS ambiente. In questa prospettiva, è possibile rispondere alle domande sia dall'alto verso il basso (ad esempio, «Quali servizi sto utilizzando per implementare i controlli di sicurezza in tutta la mia AWS organizzazione?») e dal basso verso l'alto (ad esempio, «Quali servizi gestiscono i controlli su questa istanza EC2?»). In questa sezione, analizziamo gli elementi di un AWS ambiente e identifichiamo i servizi e le funzionalità di sicurezza associati. Naturalmente, alcuni Servizi AWS dispongono di un ampio set di funzionalità e supportano diversi obiettivi di sicurezza. Questi servizi potrebbero supportare più elementi dell' AWS ambiente in uso.

Per maggiore chiarezza, forniamo brevi descrizioni di come alcuni servizi soddisfino gli obiettivi dichiarati. La sezione successiva fornisce ulteriori approfondimenti sui singoli servizi inclusi in ciascuno di essi Account AWS.

Account multipli o a livello di organizzazione

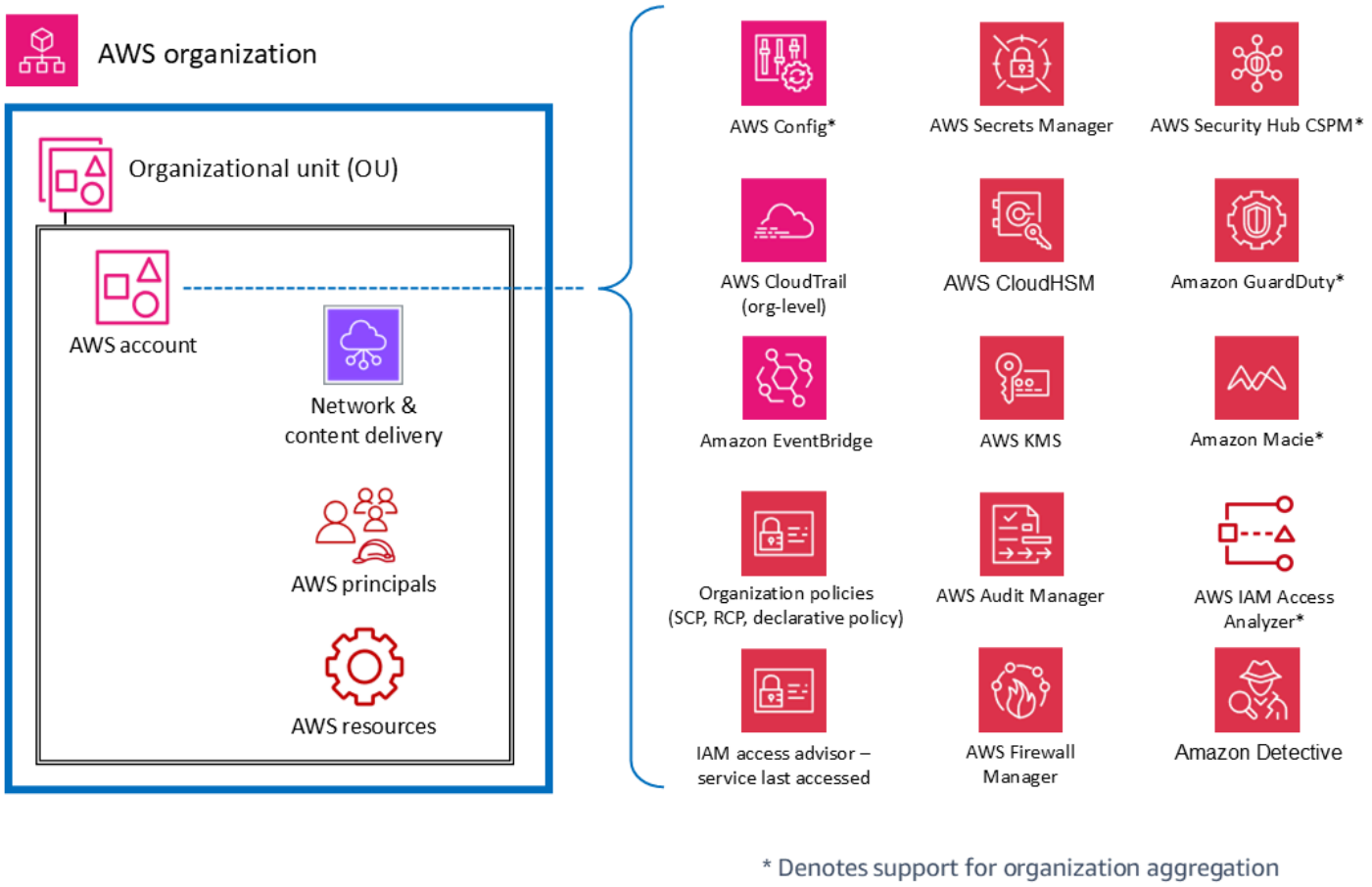
Al livello più alto, ci sono Servizi AWS funzionalità progettate per applicare funzionalità o barriere di governance e controllo su più account di un' AWS organizzazione (inclusa l'intera organizzazione o specifici). OUs Le policy di controllo dei servizi (SCPs) e le politiche di controllo delle risorse (RCPs) sono buoni esempi di funzionalità IAM che forniscono barriere preventive a livello di organizzazione. AWS AWS Organizations fornisce inoltre una politica dichiarativa che definisce e applica a livello centrale la configurazione di base su larga scala. Servizi AWS Un altro esempio è CloudTrail che fornisce il monitoraggio tramite un percorso organizzativo che registra tutti gli eventi per tutti Account AWS all'interno dell'organizzazione. AWS Questo percorso completo è distinto dai percorsi individuali che potrebbero essere creati in ciascun account. Un terzo esempio è AWS Firewall Manager che puoi utilizzare per configurare, applicare e gestire più risorse su tutti gli account della tua AWS organizzazione: AWS WAF regole, regole AWS WAF classiche, AWS Shield Advanced protezioni, gruppi di sicurezza Amazon Virtual Private Cloud (Amazon VPC) AWS Network Firewall , policy Amazon Route 53 Resolver e policy DNS Firewall.

I servizi contrassegnati da un asterisco (*) nel diagramma seguente operano con un duplice ambito: a livello di organizzazione e incentrato sull'account. Questi servizi fondamentalmente monitorano o aiutano a controllare la sicurezza all'interno di un singolo account. Tuttavia, supportano anche la possibilità di aggregare i risultati di più account in un account a livello di organizzazione per una visibilità e una gestione centralizzate. Per maggiore chiarezza, considera SCPs che si applichi a un'intera unità organizzativa o organizzazione. Account AWS AWS Al contrario, è possibile configurare e gestire GuardDuty sia a livello di account (dove vengono generati i risultati individuali) che a livello di AWS organizzazione (utilizzando la funzionalità di amministratore delegato), dove i risultati possono essere visualizzati e gestiti in forma aggregata.



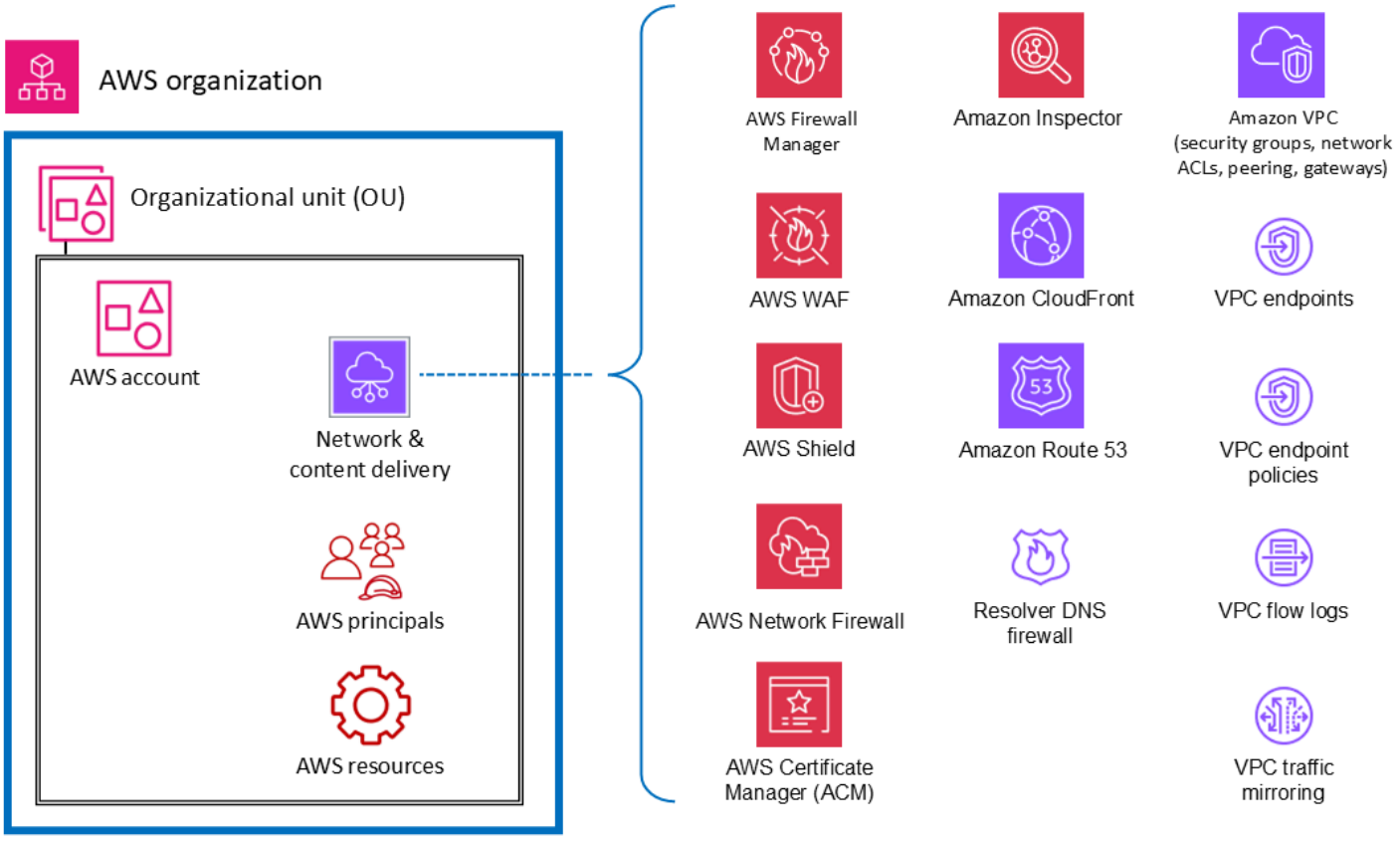
AWS conti

All'interno OUs, ci sono servizi che aiutano a proteggere più tipi di elementi all'interno di un Account AWS. Ad esempio, Gestione dei segreti AWS è spesso gestito da un account specifico e protegge le risorse (come le credenziali del database o le informazioni di autenticazione), le applicazioni e quelle Servizi AWS presenti in tale account. IAM Access Analyzer può essere configurato per generare risultati quando risorse specifiche sono accessibili da responsabili esterni a. Account AWS Come accennato nella sezione precedente, molti di questi servizi possono essere configurati e amministrati anche all'interno AWS Organizations, in modo da poter essere gestiti su più account. Questi servizi sono contrassegnati da un asterisco (*) nel diagramma. Inoltre, semplificano l'aggregazione dei risultati di più account e la loro trasmissione a un unico account. Ciò offre ai singoli team applicativi la flessibilità e la visibilità necessarie per gestire le esigenze di sicurezza specifiche del loro carico di lavoro, garantendo al contempo governance e visibilità ai team di sicurezza centralizzati. GuardDuty è un esempio di tale servizio. GuardDuty monitora le risorse e le attività associate a un singolo account e GuardDuty i risultati di più account membri (ad esempio tutti gli account di un' AWS organizzazione) possono essere raccolti, visualizzati e gestiti da un account amministratore delegato.



Rete virtuale, elaborazione e distribuzione di contenuti

Poiché l'accesso alla rete è fondamentale per la sicurezza e l'infrastruttura di elaborazione è un componente fondamentale di molti AWS carichi di lavoro, esistono molti servizi e funzionalità di AWS sicurezza dedicati a queste risorse. Ad esempio, Amazon Inspector è un servizio di gestione delle vulnerabilità che analizza continuamente i carichi di lavoro alla ricerca AWS di eventuali vulnerabilità. Queste scansioni includono controlli di raggiungibilità della rete che indicano che esistono percorsi di rete consentiti verso le istanze Amazon EC2 nel tuo ambiente. Amazon VPC ti consente di definire una rete virtuale in cui lanciare AWS risorse. Questa rete virtuale è molto simile a una rete tradizionale e include una varietà di caratteristiche e vantaggi. Gli endpoint VPC ti consentono di connettere privatamente il tuo VPC ai servizi endpoint supportati Servizi AWS e forniti da AWS PrivateLink senza richiedere un percorso verso Internet. Il diagramma seguente illustra i servizi di sicurezza che si concentrano sull'infrastruttura di rete, di elaborazione e di distribuzione dei contenuti.



Principi e risorse

AWS i principi e AWS le risorse (insieme alle politiche IAM) sono gli elementi fondamentali nella gestione delle identità e degli accessi su. AWS Un principal autenticato AWS può eseguire azioni e accedere alle AWS risorse. Un principale può essere autenticato come utente Account AWS root e utente IAM oppure assumendo un ruolo.

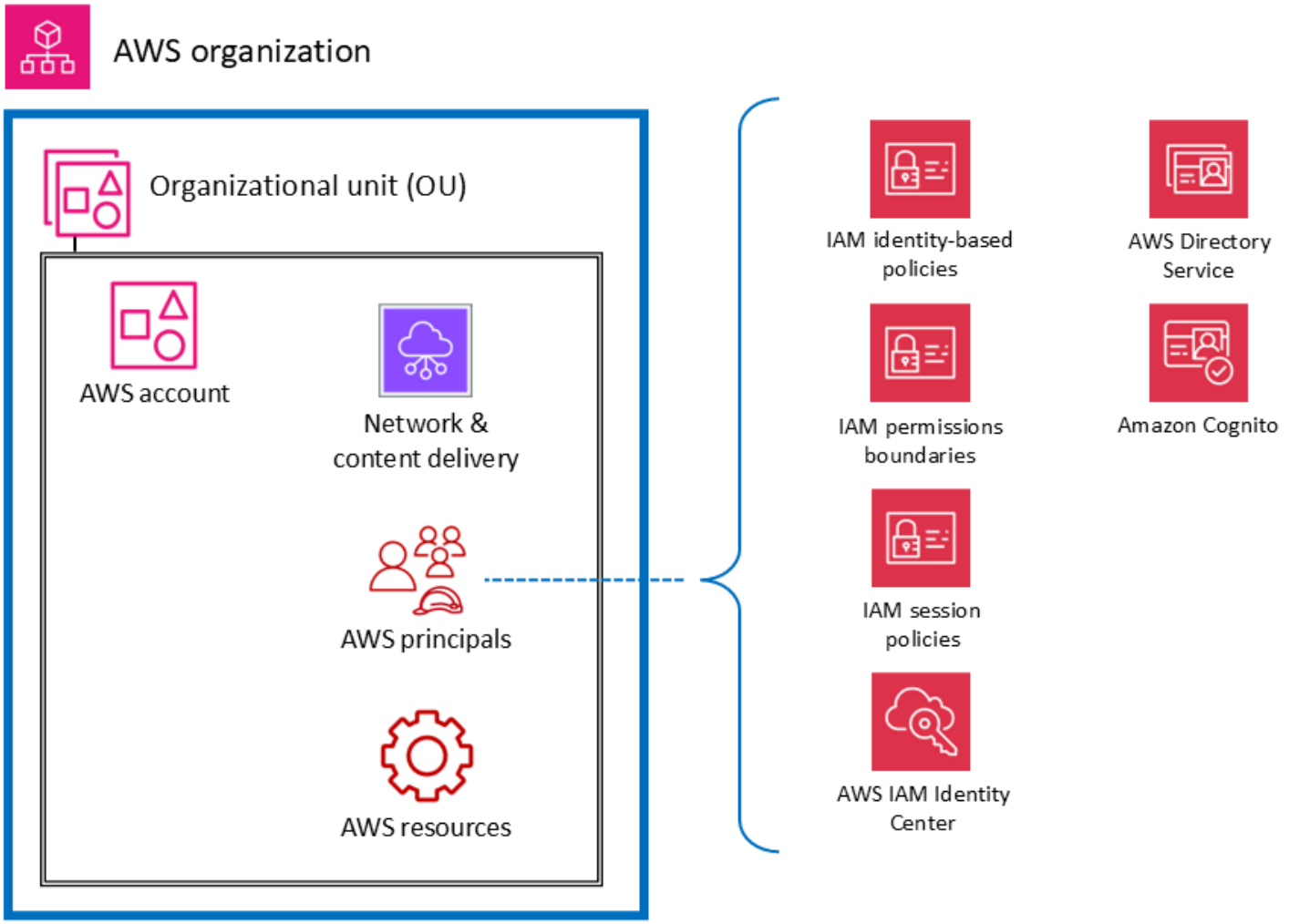
> **Note**
>
> Non create chiavi API persistenti associate all'account utente AWS root. L'accesso all'account utente root deve essere limitato solo alle attività che richiedono un utente root e solo attraverso un rigoroso processo di eccezione e approvazione. Per le migliori pratiche per proteggere l'utente root del tuo account, consulta la documentazione IAM.

Una AWS risorsa è un oggetto che esiste all'interno di un Servizio AWS oggetto su cui puoi lavorare. Gli esempi includono un'istanza EC2, uno CloudFormation stack, un argomento Amazon Simple Notification Service (Amazon SNS) e un bucket S3. Le policy IAM sono oggetti che definiscono le

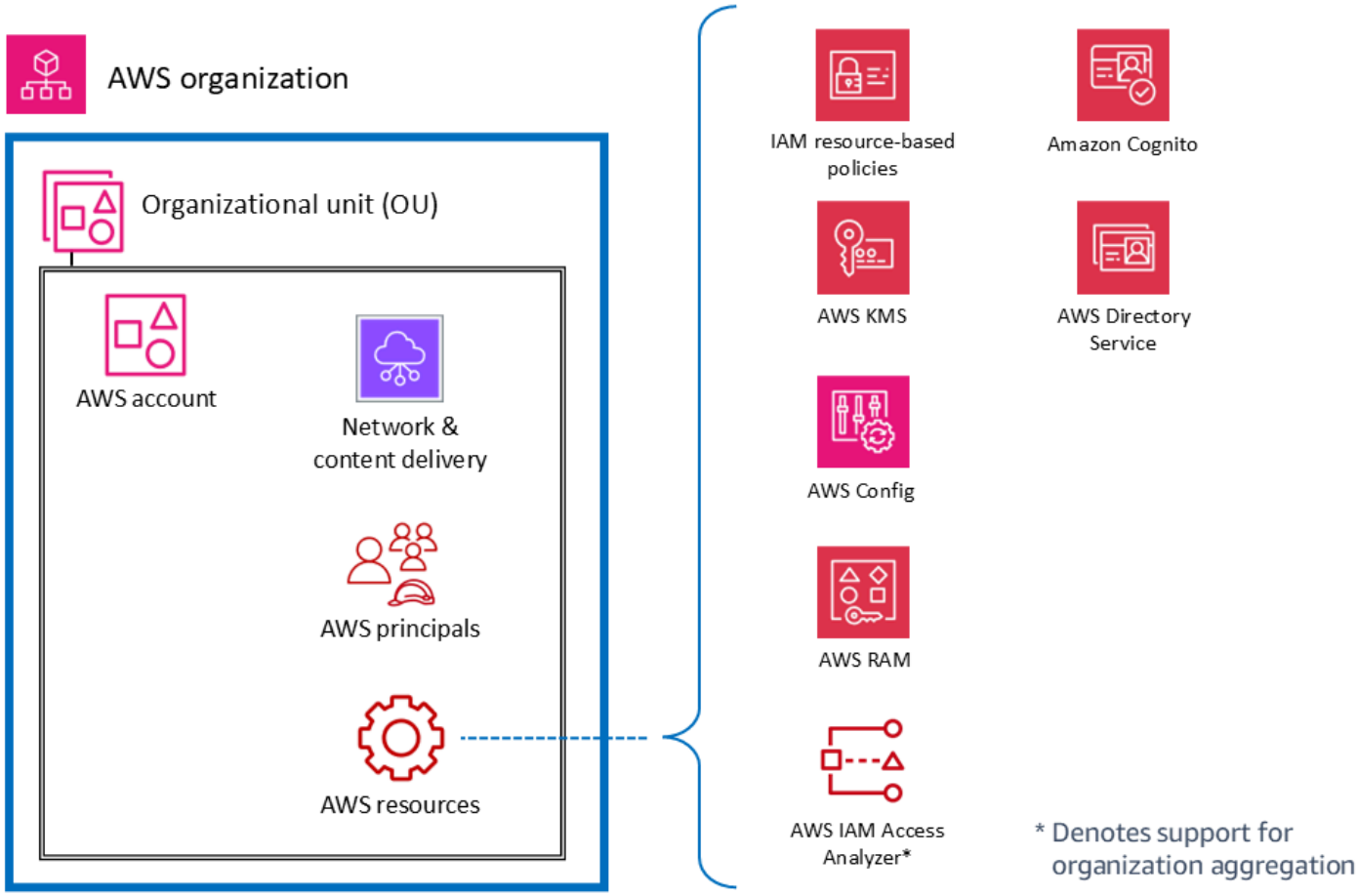
autorizzazioni quando sono associate a un principale IAM (utente, gruppo o ruolo) o a una risorsa. AWS Le policy basate sull'identità sono documenti di policy che si allegano a un principale (ruoli, utenti e gruppi di utenti) per controllare quali azioni un responsabile può eseguire, su quali risorse e in quali condizioni. Le politiche basate sulle risorse sono documenti di policy allegati a una risorsa come un bucket S3. Queste politiche concedono l'autorizzazione principale specificata per eseguire azioni specifiche su quella risorsa e definiscono le condizioni per tale autorizzazione. Le politiche basate sulle risorse sono politiche in linea. La sezione delle risorse IAM approfondisce i tipi di policy IAM e il modo in cui vengono utilizzate.

Per semplificare le cose in questa discussione, elenchiamo i servizi e le funzionalità di AWS sicurezza per i presidi IAM che hanno lo scopo principale di operare o applicare ai principali account. Manteniamo questa semplicità pur riconoscendo la flessibilità e l'ampiezza degli effetti delle politiche di autorizzazione IAM. Una singola dichiarazione in una policy può avere effetti su più tipi di entità. AWS Ad esempio, sebbene una policy basata sull'identità IAM sia associata a un principio IAM e definisca le autorizzazioni (allow, deny) per tale principale, la policy definisce implicitamente anche le autorizzazioni per le azioni, le risorse e le condizioni specificate. In questo modo, una policy basata sull'identità può essere un elemento fondamentale nella definizione delle autorizzazioni per una risorsa.

Il diagramma seguente illustra i servizi e le funzionalità di AWS sicurezza per i responsabili. AWS Le policy basate su identità sono collegate a un utente, un gruppo o un ruolo IAM. Queste policy consentono di specificare cosa può fare quell'identità (le sue autorizzazioni). Una policy di sessione IAM è una policy di autorizzazioni in linea che gli utenti passano durante la sessione quando assumono il ruolo. Puoi passare tu stesso la policy oppure puoi configurare il tuo identity broker in modo che inserisca la policy quando le tue identità vengono federate. AWS Ciò consente agli amministratori di ridurre il numero di ruoli da creare, poiché più utenti possono assumere lo stesso ruolo ma disporre di autorizzazioni di sessione uniche. Il servizio IAM Identity Center è integrato con le operazioni AWS API AWS Organizations e ti aiuta a gestire l'accesso SSO e le autorizzazioni degli utenti in tutta l'organizzazione. Account AWS AWS Organizations



Il diagramma seguente illustra i servizi e le funzionalità delle risorse dell'account. Le policy basate su risorse sono collegate a una risorsa. Ad esempio, puoi collegare policy basate sulle risorse a bucket S3, code Amazon Simple Queue Service (Amazon SQS), endpoint VPC e chiavi di crittografia. AWS KMS Puoi utilizzare politiche basate sulle risorse per specificare chi ha accesso alla risorsa e quali azioni può eseguire su di essa. Le policy dei bucket S3, le policy AWS KMS chiave e le policy degli endpoint VPC sono tipi di policy basate sulle risorse. IAM Access Analyzer ti aiuta a identificare le risorse della tua organizzazione e degli account, come i bucket S3 o i ruoli IAM, che sono condivisi con un'entità esterna. Ciò consente di identificare l'accesso involontario alle risorse e ai dati, il che rappresenta un rischio per la sicurezza. AWS Config consente di valutare, controllare e valutare le configurazioni delle AWS risorse supportate nel vostro. Account AWS AWS Config monitora e registra continuamente le configurazioni AWS delle risorse e valuta automaticamente le configurazioni registrate rispetto alle configurazioni desiderate.


AWS organization
Organizational unit (OU)
AWS account
Network & content delivery
AWS principals
AWS resources
IAM resource-based policies
Amazon Cognito
AWS KMS
AWS Directory Service
AWS Config
AWS RAM
AWS IAM Access Analyzer*
* Denotes support for organization aggregation

L'architettura AWS di riferimento per la sicurezza

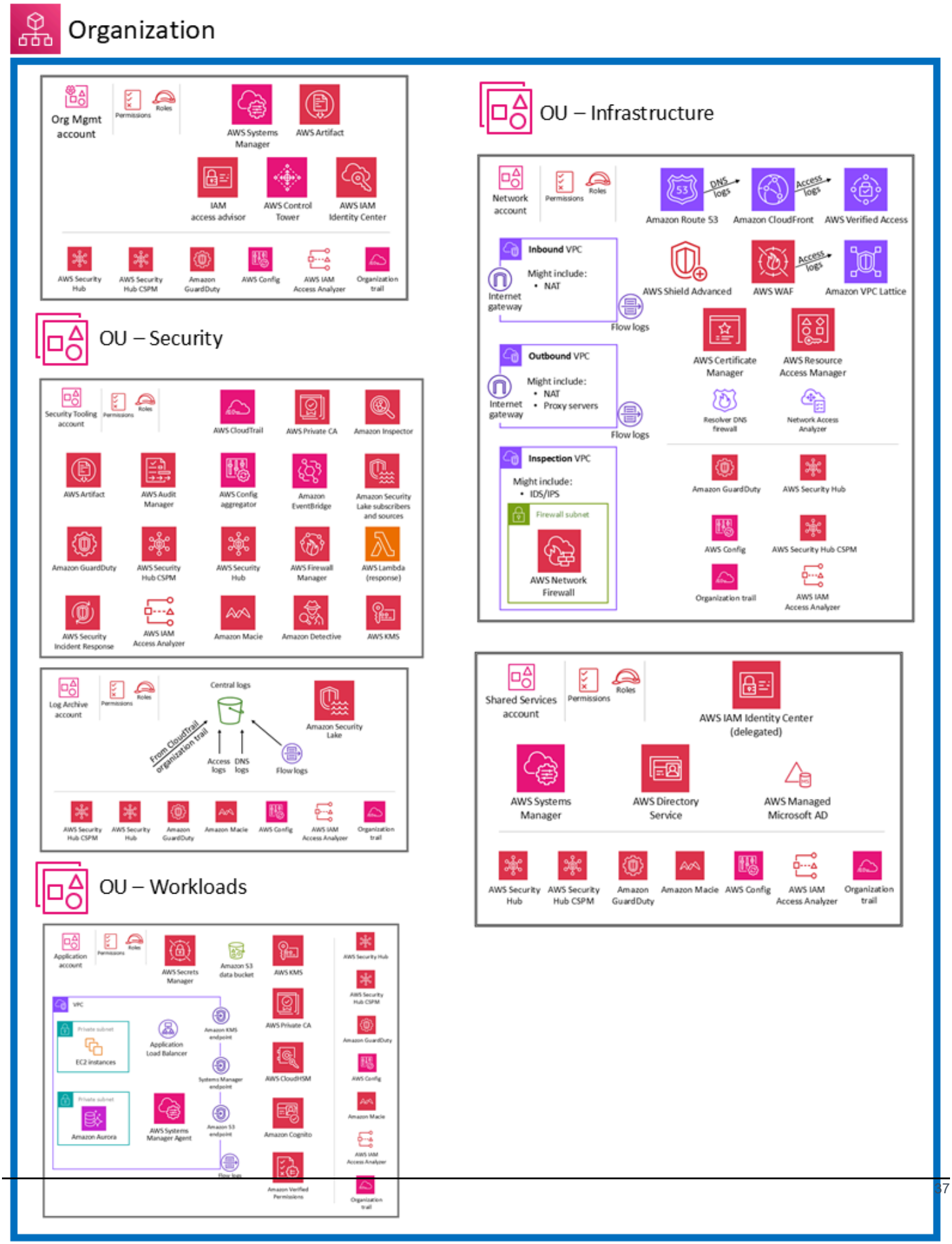
Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

Il diagramma seguente illustra la SRA. AWS Questo diagramma architettonico riunisce tutti i servizi relativi alla sicurezza. AWS È costruito attorno a una semplice architettura web a tre livelli che può essere inserita in un'unica pagina. In un simile carico di lavoro, esiste un livello web attraverso il quale gli utenti si connettono e interagiscono con il livello dell'applicazione, che gestisce l'effettiva logica aziendale dell'applicazione: riceve gli input dall'utente, esegue alcuni calcoli e genera output. Il livello dell'applicazione archivia e recupera le informazioni dal livello dati. L'architettura è volutamente modulare e fornisce un'astrazione di alto livello per molte applicazioni web moderne.

Diagrammi di architettura

Per personalizzare i diagrammi dell'architettura di riferimento di questa guida in base alle esigenze aziendali, è possibile scaricare il seguente file.zip ed estrarne il contenuto.

Scarica il file sorgente del diagramma (PowerPoint formato Microsoft)


Organization
Org Mgmt account
Permissions
Roles
AWS Systems Manager
AWS Artifact
IAM access advisor
AWS Control Tower
AWS IAM Identity Center
AWS Security Hub
AWS Security Hub CSPM
Amazon GuardDuty
AWS Config
AWS IAM Access Analyzer
Organization trail
OU – Security
Security Tooling account
AWS CloudTrail
AWS Private CA
Amazon Inspector
AWS Artifact
AWS Audit Manager
AWS Config aggregator
Amazon EventBridge
Amazon Security Lake subscribers and sources
Amazon GuardDuty
AWS Security Hub CSPM
AWS Security Hub
AWS Firewall Manager
AWS Lambda (response)
AWS Security Incident Response
AWS IAM Access Analyzer
Amazon Macie
Amazon Detective
AWS KMS
Log Archive account
Central logs
From CloudTrail, organization trail
Access logs
DNS logs
Flow logs
Amazon Security Lake
OU – Workloads
Application account
AWS Secrets Manager
Amazon S3 data bucket
AWS KMS
VPC
Private subnet
EC2 instances
Application Load Balancer
Amazon KMS endpoint
AWS Private CA
Systems Manager endpoint
AWS CloudHSM
Amazon Aurora
AWS Systems Manager Agent
Amazon S3 endpoint
Amazon Cognito
Flow logs
Amazon Verified Permissions
OU – Infrastructure
Network account
Amazon Route 53
DNS logs
Amazon CloudFront
Access logs
AWS Verified Access
Inbound VPC
Might include:
• NAT
Internet gateway
Flow logs
AWS Shield Advanced
AWS WAF
Access logs
Amazon VPC Lattice
Outbound VPC
Might include:
• NAT
• Proxy servers
Internet gateway
Flow logs
AWS Certificate Manager
AWS Resource Access Manager
Resolver DNS firewall
Network Access Analyzer
Inspection VPC
Might include:
• IDS/IPS
Firewall subnet
AWS Network Firewall
Amazon GuardDuty
AWS Security Hub
AWS Config
AWS Security Hub CSPM
Organization trail
AWS IAM Access Analyzer
Shared Services account
Permissions
Roles
AWS IAM Identity Center (delegated)
AWS Systems Manager
AWS Directory Service
AWS Managed Microsoft AD
AWS Security Hub
AWS Security Hub CSPM
Amazon GuardDuty
Amazon Macie
AWS Config
AWS IAM Access Analyzer
Organization trail

Per questa architettura di riferimento, l'applicazione Web e il livello dati effettivi sono rappresentati deliberatamente nel modo più semplice possibile, rispettivamente tramite EC2 istanze Amazon e un database Amazon Aurora. La maggior parte dei diagrammi di architettura si concentra e approfondisce i livelli Web, delle applicazioni e dei dati. Per motivi di leggibilità, spesso omettono i controlli di sicurezza. Questo diagramma ribalta tale enfasi per mostrare la sicurezza laddove possibile e mantiene i livelli di applicazione e dati tanto semplici quanto necessario per mostrare in modo significativo le funzionalità di sicurezza.

L' AWS SRA contiene tutti i servizi AWS relativi alla sicurezza disponibili al momento della pubblicazione. (Vedi cronologia dei documenti). Tuttavia, non tutti i carichi di lavoro o gli ambienti, in base alla loro esposizione unica alle minacce, devono implementare tutti i servizi di sicurezza. Il nostro obiettivo è fornire un riferimento per una serie di opzioni, comprese le descrizioni di come questi servizi si integrano tra loro dal punto di vista architettonico, in modo che la vostra azienda possa prendere le decisioni più appropriate per le vostre esigenze di infrastruttura, carico di lavoro e sicurezza, in base al rischio.

Le sezioni seguenti illustrano ciascuna unità organizzativa e account per comprenderne gli obiettivi e i singoli servizi AWS di sicurezza ad esse associati. Per ogni elemento (in genere un Servizio AWS), questo documento fornisce le seguenti informazioni:

- Breve panoramica dell'elemento e del suo scopo di sicurezza nell' AWS SRA. Per descrizioni più dettagliate e informazioni tecniche sui singoli servizi, consultare l'appendice.
- Posizionamento consigliato per abilitare e gestire il servizio nel modo più efficace. Questo viene riportato nei singoli diagrammi di architettura per ogni account e unità organizzativa.
- Collegamenti di configurazione, gestione e condivisione dei dati ad altri servizi di sicurezza. In che modo questo servizio si basa o supporta altri servizi di sicurezza?
- Considerazioni di progettazione. Innanzitutto, il documento evidenzia le funzionalità o le configurazioni opzionali che hanno importanti implicazioni in termini di sicurezza. In secondo luogo, laddove l'esperienza dei nostri team includa variazioni comuni nelle raccomandazioni che formuliamo, in genere a seguito di requisiti o vincoli alternativi, il documento descrive tali opzioni.

OUs e conti

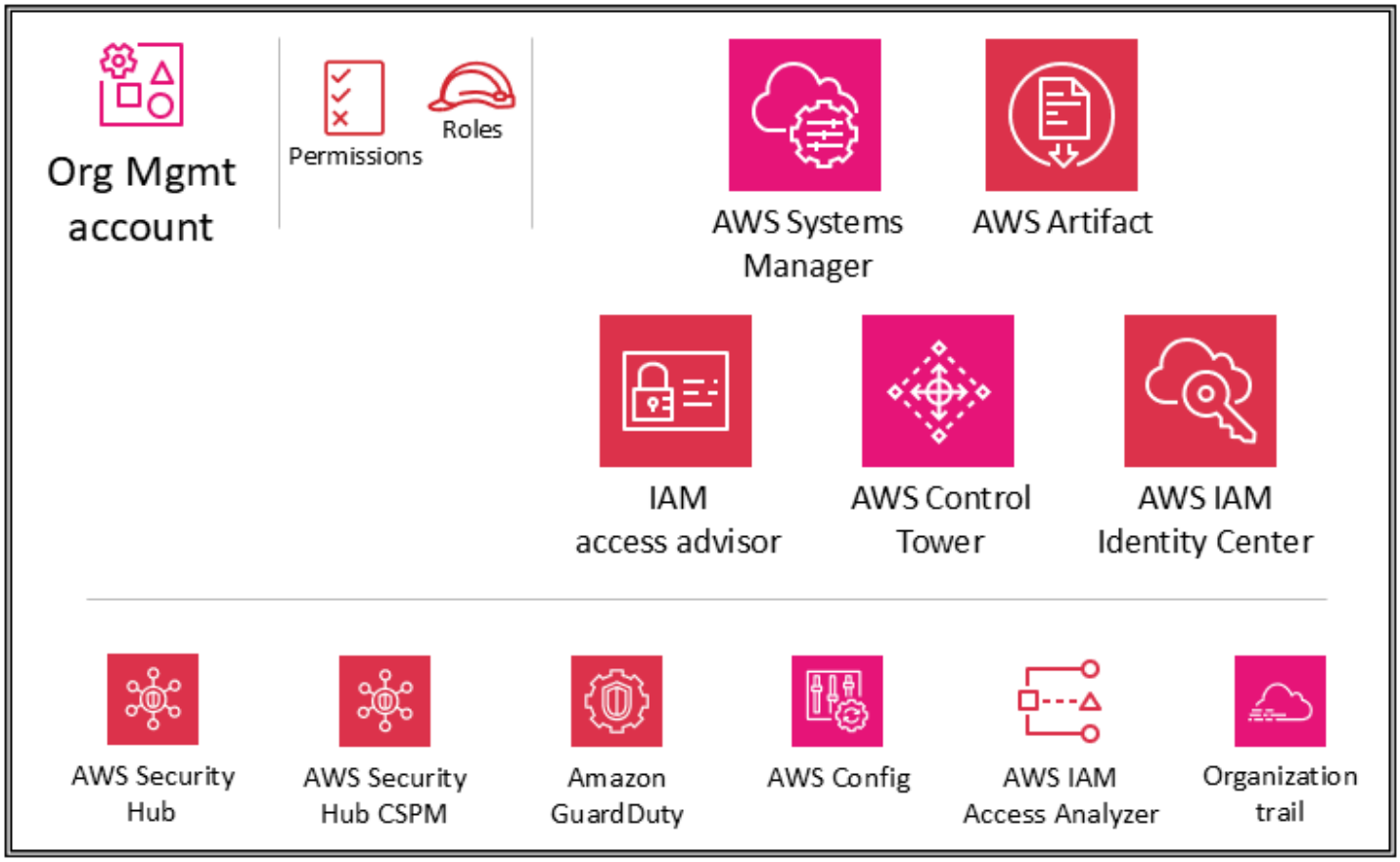
- Account di gestione dell'organizzazione
- Security OU — Account Security Tooling
- Unità organizzativa di sicurezza — Account Log Archive
- UO dell'infrastruttura - Account di rete

- Infrastruttura organizzativa — account Shared Services
- Workloads OU — Account dell'applicazione

Account di gestione dell'organizzazione

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

Il diagramma seguente illustra i servizi AWS di sicurezza configurati nell'account Org Management.



Le sezioni Utilizzo AWS Organizations per la sicurezza e L'account di gestione, l'accesso affidabile e gli amministratori delegati precedenti di questa guida hanno discusso in modo approfondito lo scopo e gli obiettivi di sicurezza dell'account di gestione dell'organizzazione. Segui le best practice di sicurezza per il tuo account di gestione dell'organizzazione. Questi includono l'utilizzo di un indirizzo e-mail gestito dall'azienda, il mantenimento delle corrette informazioni di contatto amministrative e di sicurezza (ad esempio allegando un numero di telefono all'account nel caso in cui sia AWS

necessario contattare il proprietario dell'account), l'attivazione dell'autenticazione a più fattori (MFA) per tutti gli utenti e la verifica regolare di chi ha accesso all'account di gestione dell'organizzazione. I servizi distribuiti nell'account di gestione dell'organizzazione devono essere configurati con ruoli, politiche di attendibilità e altre autorizzazioni appropriati in modo che gli amministratori di tali servizi (che devono accedervi nell'account di gestione dell'organizzazione) non possano accedere in modo inappropriato anche ad altri servizi.

Policy di controllo dei servizi

Con AWS Organizations, è possibile gestire centralmente le politiche su più livelli. Account AWS Ad esempio, è possibile applicare le politiche di controllo del servizio (SCPs) a più Account AWS membri di un'organizzazione. SCPs ti consentono di definire quali elementi Servizio AWS APIs possono e non possono essere gestiti dai responsabili IAM (come utenti e ruoli IAM) tra i membri Account AWS della tua organizzazione. SCPs vengono creati e applicati dall'account di gestione dell'organizzazione, che è Account AWS quello che hai usato quando hai creato la tua organizzazione. Per ulteriori informazioni, SCPs consulta la sezione Utilizzo AWS Organizations per la sicurezza riportata più avanti in questo riferimento.

Se gestisci AWS Control Tower la tua AWS organizzazione, questa implementerà una serie di barriere preventive (classificate SCPs come obbligatorie, fortemente consigliate o facoltative). Questi guardrail ti aiutano a gestire le tue risorse applicando i controlli di sicurezza a livello di organizzazione. Questi utilizzano SCPs automaticamente un tag con un valore di aws-control-tower. managed-by-control-tower

> **Considerazione di natura progettuale**
>
> SCPs riguardano solo gli account dei membri dell' AWS organizzazione. Sebbene vengano applicati dall'account di gestione dell'organizzazione, non hanno alcun effetto sugli utenti o sui ruoli di tale account. Per saperne di più su come funziona la logica di valutazione SCP e per vedere esempi di strutture consigliate, consultate il post AWS sul blog How to use service control policies in AWS Organizations.

Politiche di controllo delle risorse

Le politiche di controllo delle risorse (RCPs) offrono un controllo centralizzato sulle autorizzazioni massime disponibili per le risorse dell'organizzazione. Un RCP definisce una barriera di autorizzazioni o impone limiti alle azioni che le identità possono intraprendere sulle risorse

dell'organizzazione. È possibile utilizzarlo RCPs per limitare gli utenti che possono accedere alle risorse e imporre i requisiti relativi all'accesso alle risorse da parte dei membri dell'organizzazione. Account AWS Puoi collegarti RCPs direttamente ai singoli account o alla OUs cartella principale dell'organizzazione. Per una spiegazione dettagliata del RCPs funzionamento, consulta la sezione Valutazione RCP nella AWS Organizations documentazione. Per ulteriori informazioni, RCPs consulta la sezione Utilizzo AWS Organizations per la sicurezza riportata più avanti in questo riferimento.

Se gestisci AWS Control Tower la tua AWS organizzazione, questa implementerà una serie di barriere preventive (classificate RCPs come obbligatorie, fortemente consigliate o facoltative). Questi guardrail ti aiutano a gestire le tue risorse applicando i controlli di sicurezza a livello di organizzazione. Questi utilizzano SCPs automaticamente un tag con un valore di`aws-control-tower`. `managed-by-control-tower`

Considerazioni di natura progettuale

- RCPs influiscono solo sulle risorse degli account dei membri dell'organizzazione. Non hanno alcun effetto sulle risorse dell'account di gestione. Ciò significa che RCPs si applicano anche agli account dei membri designati come amministratori delegati.
- RCPs si applicano alle risorse per un sottoinsieme di. Servizi AWS Per ulteriori informazioni, consulta Elenco di Servizi AWS tale supporto RCPs nella AWS Organizations documentazione. Puoi utilizzare AWS Lambda le funzioni Regole di AWS Confige per monitorare e automatizzare l'applicazione dei controlli di sicurezza su risorse che attualmente non sono supportate da RCPs.

Policy dichiarative

Una politica dichiarativa è un tipo di politica di AWS Organizations gestione che consente di dichiarare e applicare a livello centralizzato la configurazione desiderata per un determinato elemento su larga scala Servizio AWS all'interno dell'organizzazione. Le politiche dichiarative attualmente supportano i servizi Amazon EC2, Amazon VPC e Amazon EBS. Gli attributi del servizio disponibili includono l'applicazione della versione 2 di Instance Metadata Service (IMDSv2), la risoluzione dei problemi tramite la console seriale EC2, l'autorizzazione delle impostazioni di Amazon Machine Image (AMI) e il blocco dell'accesso pubblico agli snapshot di Amazon EBS, Amazon EC2 e alle risorse Amazon VPC. AMIs Per i servizi e gli attributi supportati più recenti, consulta le politiche dichiarative nella documentazione. AWS Organizations

Puoi applicare la configurazione di base per an Servizio AWS effettuando alcune selezioni sulle AWS Control Tower console AWS Organizations e o utilizzando alcuni comandi AWS Command Line Interface ()AWS CLI e SDK. AWS Le politiche dichiarative vengono applicate nel piano di controllo del servizio, il che significa che la configurazione di base di an Servizio AWS viene sempre mantenuta, anche quando il servizio introduce nuove funzionalità o quando vengono aggiunti nuovi account a un'organizzazione o APIs quando vengono creati nuovi responsabili e risorse. Le politiche dichiarative possono essere applicate a un'intera organizzazione o a specifici account. OUs La politica efficace è l'insieme di regole ereditate dalla radice dell'organizzazione e OUs insieme alle politiche direttamente collegate all'account. Se una politica dichiarativa viene scollegata, lo stato dell'attributo tornerà allo stato precedente alla politica dichiarativa.

È possibile utilizzare politiche dichiarative per creare messaggi di errore personalizzati. Ad esempio, se un'operazione API fallisce a causa di una politica dichiarativa, è possibile impostare il messaggio di errore o fornire un URL personalizzato, ad esempio un collegamento a un wiki interno o un collegamento a un messaggio che descrive l'errore. Questo aiuta a fornire agli utenti maggiori informazioni in modo che possano risolvere il problema da soli. È inoltre possibile controllare il processo di creazione di politiche dichiarative, aggiornamento delle politiche dichiarative ed eliminazione delle politiche dichiarative utilizzando. AWS CloudTrail

Le politiche dichiarative forniscono report sullo stato degli account, che consentono di esaminare lo stato corrente di tutti gli attributi supportati dalle politiche dichiarative per gli account interessati. È possibile scegliere gli account e OUs includerli nell'ambito del rapporto oppure scegliere un'intera organizzazione selezionando la radice. Questo rapporto consente di valutare lo stato di preparazione fornendo una suddivisione per conto Regione AWS e specificando se lo stato corrente di un attributo è uniforme tra i conti (in base al `numberOfMatchedAccounts` valore) o non coerente tra i conti (in base al valore). `numberOfUnmatchedAccounts`

> **Considerazione di natura progettuale**
>
> Quando si configura un attributo di servizio utilizzando una politica dichiarativa, la politica potrebbe avere un impatto su più elementi. APIs Qualsiasi azione non conforme fallirà. Gli amministratori degli account non saranno in grado di modificare il valore dell'attributo di servizio a livello di singolo account.

Accesso root centralizzato

Tutti gli account membri AWS Organizations hanno il proprio utente root, ovvero un'identità che ha accesso completo a tutte Servizi AWS le risorse di quell'account membro. IAM offre una gestione centralizzata degli accessi root per gestire l'accesso root su tutti gli account membri. Questo aiuta a prevenire l'utilizzo da parte degli utenti root membri e aiuta a fornire il ripristino su larga scala. La funzionalità di accesso root centralizzato ha due funzionalità essenziali: gestione delle credenziali root e sessioni root.

- La funzionalità di gestione delle credenziali root consente la gestione centralizzata e aiuta a proteggere l'utente root su tutti gli account di gestione. Questa funzionalità include la rimozione delle credenziali root a lungo termine, la prevenzione del recupero delle credenziali root da parte degli account dei membri e il provisioning di nuovi account membro senza credenziali root per impostazione predefinita. Fornisce inoltre un modo semplice per dimostrare la conformità. Quando la gestione degli utenti root è centralizzata, è possibile rimuovere le password degli utenti root, le chiavi di accesso e i certificati di firma e disattivare l'autenticazione a più fattori (MFA) da tutti gli account membri.
- La funzionalità delle sessioni root consente di eseguire azioni utente root privilegiate utilizzando credenziali a breve termine sugli account dei membri provenienti dall'account di gestione dell'organizzazione o dagli account amministratore delegati. Questa funzionalità consente di abilitare l'accesso root a breve termine limitato a azioni specifiche, in conformità al principio del privilegio minimo.

Per la gestione centralizzata delle credenziali root, è necessario abilitare le funzionalità di gestione delle credenziali root e delle sessioni root a livello di organizzazione dall'account di gestione dell'organizzazione o in un account amministratore delegato. Seguendo le best practice AWS SRA, deleghiamo questa funzionalità all'account Security Tooling. Per informazioni sulla configurazione e l'utilizzo dell'accesso centralizzato degli utenti root, consultate il post del blog sulla AWS sicurezza, Gestire centralmente l'accesso root per i clienti che utilizzano. AWS Organizations

Centro identità IAM

AWS IAM Identity Centerè un servizio di federazione delle identità che ti aiuta a gestire centralmente l'accesso SSO a tutti i tuoi carichi di Account AWS lavoro, principali e cloud. IAM Identity Center ti aiuta anche a gestire l'accesso e le autorizzazioni alle applicazioni SaaS (Software as a Service) di terze parti di uso comune. I provider di identità si integrano con IAM Identity Center utilizzando SAML 2.0. Il bulk e il just-in-time provisioning possono essere eseguiti utilizzando il System for

Cross-Domain Identity Management (SCIM). IAM Identity Center può anche integrarsi con domini AWS Microsoft Active Directory (AD) locali o gestiti come provider di identità tramite l'uso di. AWS Directory Service IAM Identity Center include un portale utenti in cui gli utenti finali possono trovare e accedere all' Account AWS IAM Identity Center, ai ruoli, alle applicazioni cloud e alle applicazioni personalizzate assegnati in un unico posto.

Per impostazione predefinita, IAM Identity Center si integra nativamente AWS Organizations e viene eseguito nell'account Org Management. Tuttavia, per esercitare il minimo privilegio e controllare rigorosamente l'accesso all'account di gestione, l'amministrazione di IAM Identity Center può essere delegata a un account membro specifico. Nell' AWS SRA, l'account Shared Services è l'account amministratore delegato per IAM Identity Center. Prima di abilitare l'amministrazione delegata per IAM Identity Center, esamina queste considerazioni. Ulteriori informazioni sulla delega sono disponibili nella sezione relativa all'account di Shared Services. Anche dopo aver abilitato la delega, IAM Identity Center deve comunque essere eseguito nell'account di gestione dell'organizzazione per eseguire determinate attività relative a IAM Identity Center, tra cui la gestione dei set di autorizzazioni forniti nell'account di gestione dell'organizzazione.

All'interno della console IAM Identity Center, gli account vengono visualizzati in base all'unità organizzativa incapsulata. Ciò consente di scoprire rapidamente le proprie autorizzazioni Account AWS, applicare set comuni di autorizzazioni e gestire l'accesso da una posizione centrale.

IAM Identity Center include un archivio di identità in cui devono essere archiviate informazioni utente specifiche. Tuttavia, IAM Identity Center non deve essere la fonte autorevole per le informazioni sulla forza lavoro. Nei casi in cui l'azienda dispone già di una fonte autorevole, IAM Identity Center supporta i seguenti tipi di provider di identità (). IdPs

- IAM Identity Center identity store: scegli questa opzione se le seguenti due opzioni non sono disponibili. Gli utenti vengono creati, le assegnazioni ai gruppi e le autorizzazioni vengono assegnate nell'archivio di identità. Anche se la fonte autorevole è esterna a IAM Identity Center, una copia degli attributi principali verrà archiviata nell'archivio di identità.
- Microsoft Active Directory (AD): scegli questa opzione se desideri continuare a gestire gli utenti nella tua directory in AWS Directory Service for Microsoft Active Directory o nella directory autogestita in Active Directory.
- Provider di identità esterno: scegli questa opzione se preferisci gestire gli utenti in un IdP esterno di terze parti basato su SAML.

Puoi fare affidamento su un IdP esistente già presente all'interno della tua azienda. Ciò semplifica la gestione dell'accesso su più applicazioni e servizi, poiché l'accesso viene creato, gestito e revocato da un'unica posizione. Ad esempio, se qualcuno lascia il tuo team, puoi revocare il suo accesso a tutte le applicazioni e i servizi (inclusi Account AWS) da un'unica posizione. Ciò riduce la necessità di più credenziali e offre l'opportunità di integrarsi con i processi relativi alle risorse umane (HR).

> Considerazione di natura progettuale
>
> Utilizza un IdP esterno se tale opzione è disponibile per la tua azienda. Se il tuo IdP supporta System for Cross-domain Identity Management (SCIM), sfrutta la funzionalità SCIM di IAM Identity Center per automatizzare il provisioning (sincronizzazione) di utenti, gruppi e autorizzazioni. Ciò consente ad AWS Access di rimanere sincronizzato con il flusso di lavoro aziendale per i nuovi assunti, i dipendenti che si trasferiscono in un altro team e i dipendenti che lasciano l'azienda. In qualsiasi momento, puoi avere solo una directory o un provider di identità SAML 2.0 connesso a IAM Identity Center. Tuttavia, puoi passare a un altro provider di identità.

Consulente di accesso IAM

IAM access advisor fornisce dati di tracciabilità sotto forma di informazioni sull'ultimo accesso al servizio per te Account AWS e. OUs Usa questo controllo investigativo per contribuire a una strategia con privilegi minimi. Per i responsabili IAM, puoi visualizzare due tipi di informazioni sull'ultimo accesso: informazioni consentite e Servizio AWS informazioni sulle azioni consentite. Le informazioni includono la data e l'ora in cui è stato effettuato il tentativo.

L'accesso IAM all'interno dell'account Org Management consente di visualizzare i dati dell'ultimo accesso al servizio per l'account Org Management, l'unità organizzativa, l'account membro o la politica IAM AWS dell'organizzazione. Queste informazioni sono disponibili nella console IAM all'interno dell'account di gestione e possono anche essere ottenute a livello di codice utilizzando IAM Access Advisor APIs in AWS CLI o un client programmatico. Le informazioni indicano quali entità di un'organizzazione o di un account hanno tentato l'ultimo accesso al servizio e quando. Le informazioni sull'ultimo accesso forniscono informazioni sull'utilizzo effettivo del servizio (vedi scenari di esempio), in modo da poter ridurre le autorizzazioni IAM solo ai servizi effettivamente utilizzati.

AWS Systems Manager

Quick Setup ed Explorer, che sono funzionalità di AWS Systems Manager, supportano AWS Organizations e operano dall'account di gestione dell'organizzazione.

Quick Setup è una funzionalità di automazione di Systems Manager. Consente all'account Org Management di definire facilmente le configurazioni per consentire a Systems Manager di intervenire per conto dell'utente tra gli account AWS dell'organizzazione. È possibile abilitare la configurazione rapida in tutta l' AWS organizzazione o sceglierne di specifiche OUs. Quick Setup può pianificare AWS Systems Manager l'agente (agente SSM) per eseguire aggiornamenti bisettimanali sulle istanze EC2 e può impostare una scansione giornaliera di tali istanze per identificare le patch mancanti.

Explorer è una dashboard operativa personalizzabile che riporta informazioni sulle tue risorse. AWS Explorer mostra una visualizzazione aggregata dei dati operativi per i tuoi AWS account e per tutti Regioni AWS gli altri. Ciò include i dati sulle istanze EC2 e i dettagli sulla conformità delle patch. Dopo aver completato la configurazione integrata (che include anche Systems Manager OpsCenter) all'interno AWS Organizations, è possibile aggregare i dati in Explorer per unità organizzativa o per un'intera AWS organizzazione. Systems Manager aggrega i dati nell'account AWS Org Management prima di visualizzarli in Explorer.

La sezione Workloads OU più avanti in questa guida illustra l'uso dell'agente SSM sulle istanze EC2 nell'account dell'applicazione.

AWS Control Tower

AWS Control Toweroffre un modo semplice per configurare e gestire un AWS ambiente sicuro con più account, chiamato landing zone. AWS Control Tower crea la tua landing zone utilizzando AWS Organizations e fornisce una gestione e una governance degli account continue, nonché le migliori pratiche di implementazione. Puoi utilizzarlo AWS Control Tower per fornire nuovi account in pochi passaggi, assicurandoti al contempo che gli account siano conformi alle politiche organizzative. Puoi persino aggiungere account esistenti a un nuovo AWS Control Tower ambiente.

AWS Control Tower dispone di un set di funzionalità ampio e flessibile. Una caratteristica fondamentale è la sua capacità di orchestrare le funzionalità di molti altri Servizi AWS AWS Organizations, AWS Service Catalog tra cui IAM Identity Center, per creare una landing zone. Ad esempio, per impostazione predefinita AWS Control Tower utilizza per AWS CloudFormation stabilire una linea di base, politiche di controllo del AWS Organizations servizio (SCPs) per prevenire modifiche alla configurazione e Regole di AWS Config regole per rilevare continuamente

le non conformità. AWS Control Tower utilizza progetti che consentono di allineare rapidamente l' AWS ambiente multi-account ai principi di progettazione delle basi di sicurezza di Well Architected.AWS Tra le funzionalità di governance, AWS Control Tower offre barriere che impediscono l'implementazione di risorse non conformi a politiche selezionate.

Puoi iniziare a implementare le linee guida AWS SRA con. AWS Control Tower Ad esempio, AWS Control Tower crea un' AWS organizzazione con l'architettura multi-account consigliata. Fornisce progetti per fornire la gestione delle identità, fornire l'accesso federato agli account, centralizzare la registrazione, stabilire controlli di sicurezza su più account, definire un flusso di lavoro per il provisioning di nuovi account e implementare le linee di base degli account con le configurazioni di rete.

In AWS SRA, AWS Control Tower rientra nell'account di gestione dell'organizzazione perché AWS Control Tower utilizza questo account per configurare automaticamente un' AWS organizzazione e designa tale account come account di gestione. Questo account viene utilizzato per la fatturazione all'interno dell'organizzazione. AWS Viene anche utilizzato per la fornitura di account da parte di Account Factory, per gestire OUs e gestire i guardrail. Se si esegue l'avvio AWS Control Tower in un' AWS organizzazione esistente, è possibile utilizzare l'account di gestione esistente. AWS Control Tower utilizzerà quell'account come account di gestione designato.

> **Considerazione di natura progettuale**
>
> Se desideri eseguire ulteriori operazioni di base dei controlli e delle configurazioni dei tuoi account, puoi utilizzare Customizations for AWS Control Tower (cFCT). Con cFct, puoi personalizzare la tua AWS Control Tower landing zone utilizzando un CloudFormation modello e SCPs. Puoi distribuire il modello e le politiche personalizzati su singoli account e OUs all'interno della tua organizzazione. cFCT si integra con gli eventi AWS Control Tower del ciclo di vita per garantire che l'implementazione delle risorse rimanga sincronizzata con la landing zone.

AWS Artifact

AWS Artifactfornisce accesso su richiesta ai report di AWS sicurezza e conformità e ad accordi online selezionati. I report disponibili AWS Artifact includono report SOC (System and Organization Controls), report PCI (Payment Card Industry) e certificazioni di organismi di accreditamento di diverse aree geografiche e verticali di conformità che convalidano l'implementazione e l'efficacia operativa dei controlli di sicurezza. AWS AWS Artifact vi aiuta a svolgere la due diligence con una

maggiore trasparenza nel nostro ambiente di controllo della sicurezza AWS . Inoltre, consente di monitorare continuamente la sicurezza e la conformità AWS con accesso immediato ai nuovi report.

AWS Artifact Gli accordi consentono di esaminare, accettare e tenere traccia dello stato di AWS accordi come il Business Associate Addendum (BAA) per un singolo account e per gli account di cui fanno parte dell'organizzazione. AWS Organizations

È possibile fornire gli elementi di AWS controllo ai revisori o alle autorità di regolamentazione come prova dei controlli di sicurezza. AWS Puoi anche utilizzare le indicazioni sulla responsabilità fornite da alcuni degli elementi di AWS audit per progettare la tua architettura cloud. Questa guida aiuta a determinare i controlli di sicurezza aggiuntivi che è possibile mettere in atto per supportare i casi d'uso specifici del sistema.

AWS Artifact è ospitato nell'account di gestione dell'organizzazione per fornire una posizione centrale in cui è possibile rivedere, accettare e gestire gli accordi con AWS. Questo perché gli accordi accettati nell'account di gestione confluiscono negli account dei membri.

> **Considerazione di natura progettuale**
>
> Gli utenti all'interno dell'account di gestione dell'organizzazione devono essere limitati a utilizzare solo la funzionalità Accordi AWS Artifact e nient'altro. Per implementare la separazione delle mansioni, AWS Artifact è anche ospitata nell'account Security Tooling, dove è possibile delegare le autorizzazioni alle parti interessate alla conformità e ai revisori esterni per accedere agli artefatti di controllo. È possibile implementare questa separazione definendo politiche di autorizzazione IAM granulari. Per alcuni esempi, consulta Esempi di politiche IAM nella documentazione. AWS

Guardrail dei servizi di sicurezza distribuiti e centralizzati

In AWS SRA,,, Amazon AWS Security Hub AWS Security Hub CSPM GuardDuty, AWS Config IAM Access Analyzer, gli itinerari AWS CloudTrail organizzativi e spesso Amazon Macie vengono distribuiti con un set di barriere delegate appropriato tra gli account e forniscono anche monitoraggio, gestione e governance centralizzati in tutta l'organizzazione. AWS Troverai questo gruppo di servizi in ogni tipo di account rappresentato nell'SRA. AWS Questi dovrebbero far parte di Servizi AWS ciò che deve essere fornito nell'ambito del processo di registrazione e baselining dell'account. L'archivio del GitHub codice fornisce un esempio di implementazione di servizi AWS incentrati sulla sicurezza in tutti gli account, incluso l'account di gestione dell'organizzazione. AWS

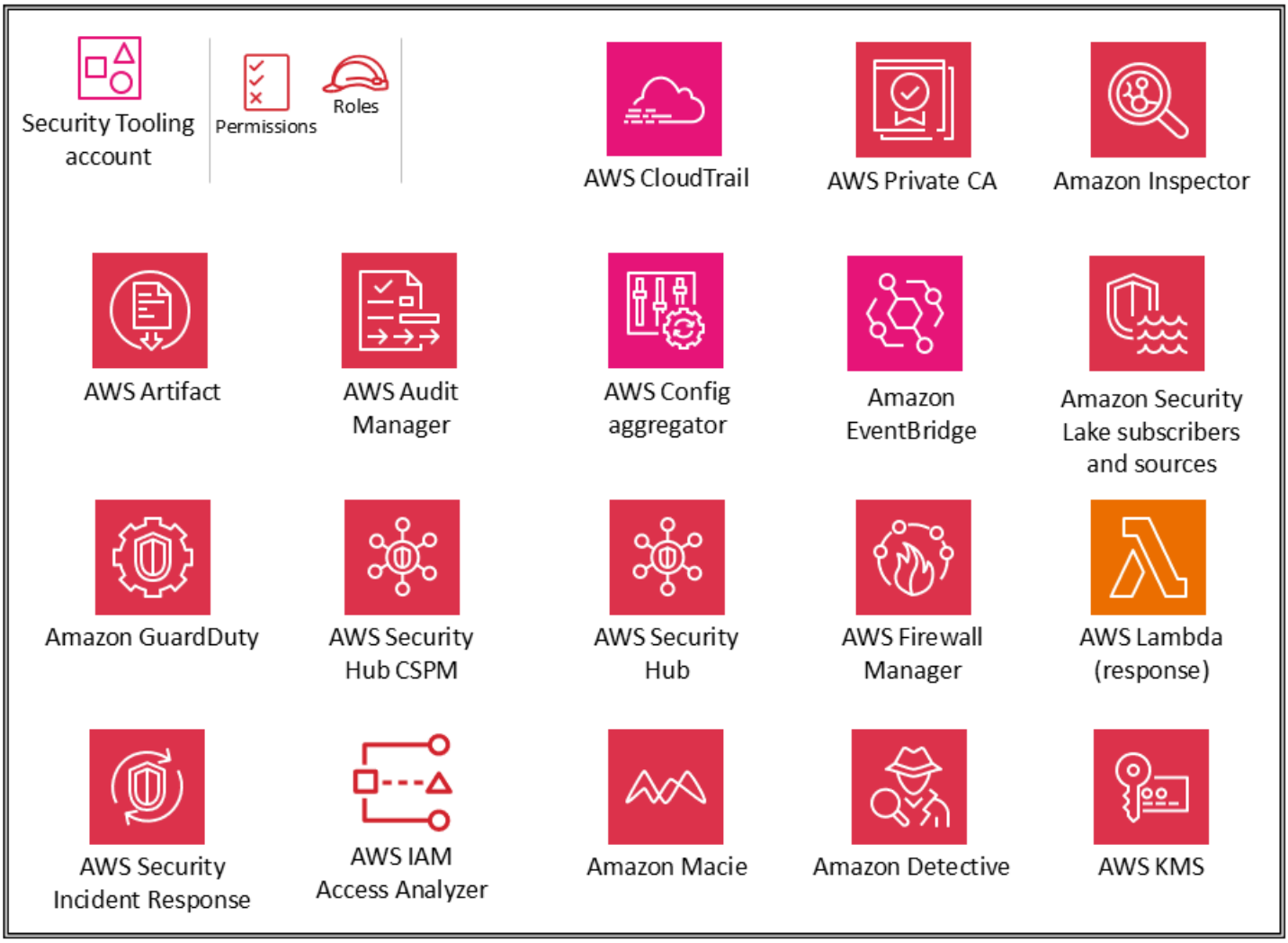
Oltre a questi servizi, AWS SRA include due servizi incentrati sulla sicurezza, Amazon Detective e AWS Audit Manager, che supportano l'integrazione e la funzionalità di amministratore delegato in. AWS Organizations Tuttavia, questi non sono inclusi tra i servizi consigliati per la baseline degli account. Abbiamo visto che questi servizi vengono utilizzati al meglio nei seguenti scenari:

- Disponi di un team o di un gruppo di risorse dedicato che svolgono tali funzioni di analisi forense digitale e audit IT. Detective viene utilizzato al meglio dai team di analisti della sicurezza e Audit Manager è utile per i team interni di audit o conformità.
- Desideri concentrarti su un set di strumenti di base come AWS Config Amazon e GuardDuty AWS Security Hub, AWS Security Hub CSPM all'inizio del tuo progetto, per poi sfruttare questi strumenti utilizzando servizi che forniscono funzionalità aggiuntive.

Security OU — Account Security Tooling

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

Il diagramma seguente illustra i servizi AWS di sicurezza configurati nell'account Security Tooling.



L'account Security Tooling è dedicato alla gestione dei servizi di sicurezza, al monitoraggio Account AWS e all'automazione degli avvisi e delle risposte di sicurezza. Gli obiettivi di sicurezza includono i seguenti:

- Fornisci un account dedicato con accesso controllato per gestire l'accesso alle barriere di sicurezza, il monitoraggio e la risposta.
- Mantieni l'infrastruttura di sicurezza centralizzata appropriata per monitorare i dati delle operazioni di sicurezza e mantenere la tracciabilità. Il rilevamento, l'indagine e la risposta sono parti essenziali del ciclo di vita della sicurezza e possono essere utilizzati per supportare un processo di qualità, un obbligo legale o di conformità e per l'identificazione e la risposta alle minacce.
- Supporta ulteriormente una strategia defense-in-depth organizzativa mantenendo un altro livello di controllo sulla configurazione e sulle operazioni di sicurezza appropriate, come le chiavi di crittografia e le impostazioni dei gruppi di sicurezza. Questo è un account in cui lavorano gli

operatori di sicurezza. I ruoli di sola lettura/controllo per visualizzare le informazioni a AWS livello di organizzazione sono tipici, mentre i write/modify ruoli sono in numero limitato, strettamente controllati, monitorati e registrati.

Considerazioni di natura progettuale

- AWS Control Tower per impostazione predefinita, assegna all'account dell'unità organizzativa di sicurezza il nome Account di controllo. È possibile rinominare l'account durante la AWS Control Tower configurazione.
- Potrebbe essere opportuno avere più di un account Security Tooling. Ad esempio, il monitoraggio e la risposta agli eventi di sicurezza vengono spesso assegnati a un team dedicato. La sicurezza della rete potrebbe richiedere un account e ruoli propri in collaborazione con l'infrastruttura cloud o il team di rete. Tali divisioni mantengono l'obiettivo di separare le enclave di sicurezza centralizzate e enfatizzano ulteriormente la separazione dei compiti, il privilegio minimo e la potenziale semplicità delle assegnazioni dei team. Se si utilizza AWS Control Tower, limita la creazione di ulteriori elementi nell'unità organizzativa di sicurezza. Account AWS

Amministratore delegato per i servizi di sicurezza

L'account Security Tooling funge da account amministratore per i servizi di sicurezza gestiti in una administrator/member struttura in tutto il. Account AWS Come accennato in precedenza, questo viene gestito tramite la funzionalità di amministratore AWS Organizations delegato. I servizi dell' AWS SRA che attualmente supportano l'amministratore delegato includono la gestione centralizzata IAM dell'accesso root,, AWS Firewall Manager Amazon AWS Config, IAM Access Analyzer GuardDuty, Amazon Macie,, Amazon AWS Security Hub Detective, AWS Security Hub CSPM AWS Audit Manager Amazon Inspector e. AWS CloudTrail AWS Systems Manager Il tuo team di sicurezza gestisce le funzionalità di sicurezza di questi servizi e monitora eventuali eventi o risultati specifici relativi alla sicurezza.

AWS IAM Identity Center supporta l'amministrazione delegata di un account membro. AWS SRA utilizza l'account Shared Services come account amministratore delegato per IAM Identity Center, come spiegato più avanti nella sezione IAM Identity Center dell'account Shared Services.

Accesso root centralizzato

L'account Security Tooling è l'account amministratore delegato per la gestione centralizzata IAM della funzionalità di accesso root. Questa funzionalità deve essere abilitata a livello di organizzazione abilitando la gestione delle credenziali e l'azione root privilegiata negli account dei membri. Agli amministratori delegati devono essere fornite esplicitamente `sts:AssumeRoot` le autorizzazioni per poter eseguire azioni root privilegiate per conto degli account dei membri. Questa autorizzazione è disponibile solo dopo che l'azione root privilegiata in un account membro è stata abilitata nell'account di gestione dell'organizzazione o nell'account amministratore delegato. Con questa autorizzazione, gli utenti possono eseguire attività di utente root privilegiato sugli account dei membri, centralmente dall'account Security Tooling. Dopo aver avviato una sessione privilegiata, è possibile eliminare una policy del bucket S3 non configurata correttamente, eliminare una politica di coda SQS non configurata correttamente, eliminare le credenziali dell'utente root per un account membro e riattivare le credenziali dell'utente root per un account membro. È possibile eseguire queste azioni dalla console, utilizzando () o tramite. AWS Command Line Interface AWS CLI APIs

AWS CloudTrail

AWS CloudTrailè un servizio che supporta la governance, la conformità e il controllo delle attività nel tuo Account AWS. Con CloudTrail, puoi registrare, monitorare continuamente e conservare le attività dell'account relative alle azioni sull' AWS infrastruttura. CloudTrail è integrato con AWS Organizations e tale integrazione può essere utilizzata per creare un unico percorso che registra tutti gli eventi per tutti gli account dell' AWS organizzazione. Questo tipo di trail viene indicato come trail dell'organizzazione. È possibile creare e gestire un percorso organizzativo solo dall'interno dell'account di gestione dell'organizzazione o da un account amministratore delegato. Quando si crea un percorso organizzativo, viene creato un percorso con il nome specificato in ogni percorso Account AWS che appartiene all' AWS organizzazione. Il trail registra l'attività di tutti gli account, incluso l'account di gestione, dell' AWS organizzazione e archivia i log in un unico bucket S3. Data la sensibilità di questo bucket S3, dovresti proteggerlo seguendo le best practice descritte nella sezione Amazon S3 come archivio di log centrale più avanti in questa guida. Tutti gli account AWS dell'organizzazione possono visualizzare il percorso dell'organizzazione nel proprio elenco di percorsi. Tuttavia, i membri Account AWS hanno accesso in sola visualizzazione a questo percorso. Per impostazione predefinita, quando si crea un percorso organizzativo nella CloudTrail console, il percorso è un percorso multiregionale. Per ulteriori best practice di sicurezza, consulta la CloudTraildocumentazione.

In AWS SRA, l'account Security Tooling è l'account amministratore delegato per la gestione. CloudTrail Il bucket S3 corrispondente per archiviare i log dell'organizzazione viene creato nell'account Log Archive. Questo serve a separare la gestione e l'utilizzo dei privilegi di CloudTrail registro. Per informazioni su come creare o aggiornare un bucket S3 per archiviare i file di registro per un percorso organizzativo, consulta la documentazione. CloudTrail Come best practice di sicurezza, aggiungi la chiave di `aws:SourceArn` condizione dell'organigramma alla politica delle risorse del bucket S3 (e a qualsiasi altra risorsa come le chiavi KMS o gli argomenti SNS). Ciò garantisce che il bucket S3 accetti solo i dati associati al percorso specifico. Il percorso è configurato con la convalida dei file di registro per la convalida dell'integrità dei file di registro. I file di log e digest vengono crittografati utilizzando SSE-KMS. L'organigramma è inoltre integrato con un gruppo di log in CloudWatch Logs per inviare eventi per la conservazione a lungo termine.

> **Note**
>
> È possibile creare e gestire gli itinerari organizzativi sia dagli account di gestione che dagli account di amministratore delegato. Tuttavia, come best practice, è necessario limitare l'accesso all'account di gestione e utilizzare la funzionalità di amministratore delegato laddove disponibile.

> **Considerazioni di natura progettuale**
>
> - CloudTrail per impostazione predefinita, non registra gli eventi relativi ai dati, poiché si tratta spesso di attività ad alto volume. Tuttavia, è necessario acquisire gli eventi relativi ai dati per AWS risorse critiche specifiche come i bucket S3, le funzioni Lambda, gli eventi di registro dall'esterno AWS che vengono inviati al CloudTrail lago e gli argomenti SNS. A tale scopo, configura il percorso organizzativo in modo che includa gli eventi relativi ai dati provenienti da risorse specifiche specificando le singole risorse. ARNs
> - Se un account membro richiede l'accesso ai file di CloudTrail registro per il proprio account, puoi condividere selettivamente i file di CloudTrail registro dell'organizzazione dal bucket S3 centrale. Tuttavia, se gli account membri richiedono gruppi di CloudWatch log Amazon locali per CloudTrail i log del proprio account o desiderano configurare la gestione dei log e gli eventi relativi ai dati (sola lettura, sola scrittura, eventi di gestione, eventi relativi ai dati) in modo diverso dall'organigramma, possono creare un percorso locale con i controlli appropriati. I percorsi locali specifici per account comportano costi aggiuntivi.

AWS Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM), precedentemente noto come AWS Security Hub, ti offre una visione completa del tuo livello di sicurezza e ti aiuta a controllare il tuo ambiente rispetto agli AWS standard e alle migliori pratiche del settore della sicurezza. Security Hub CSPM raccoglie dati di sicurezza da servizi AWS integrati, prodotti di terze parti supportati e altri prodotti di sicurezza personalizzati che potresti utilizzare. Aiuta a monitorare e analizzare costantemente le tendenze di sicurezza e a identificare i problemi di sicurezza più importanti. Oltre alle fonti acquisite, Security Hub CSPM genera i propri risultati, che sono rappresentati da controlli di sicurezza mappati a uno o più standard di sicurezza. Questi standard includono AWS Foundational Security Best Practices (FSBP), Center for Internet Security (CIS) AWS Foundations Benchmark v1.20 e v1.4.0, National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5, Payment Card Industry Data Security Standard (PCI DSS) e standard di gestione dei servizi. Per un elenco degli standard di sicurezza attuali e dettagli su controlli di sicurezza specifici, vedere il riferimento agli standard per Security Hub CSPM nella documentazione CSPM di Security Hub.

Security Hub CSPM si integra AWS Organizations per semplificare la gestione del livello di sicurezza su tutti gli account esistenti e futuri dell'organizzazione. AWS È possibile utilizzare la funzionalità di configurazione centrale CSPM di Security Hub dall'account amministratore delegato (in questo caso, Security Tooling) per specificare in che modo il servizio CSPM di Security Hub, gli standard di sicurezza e i controlli di sicurezza sono configurati negli account e nelle unità organizzative dell'organizzazione () tra le regioni. OUs È possibile configurare queste impostazioni in pochi passaggi da una regione principale, denominata regione di origine. Se non utilizzi la configurazione centrale, devi configurare Security Hub CSPM separatamente in ogni account e regione. L'amministratore delegato può designare account e OUs gestirli autonomamente, in cui il membro può configurare le impostazioni separatamente in ciascuna regione, oppure gestirli centralmente, in cui l'amministratore delegato può configurare l'account membro o l'unità organizzativa tra le regioni. È possibile designare tutti gli account e OUs quelli dell'organizzazione come gestiti centralmente, tutti autogestiti o una combinazione di entrambi. Ciò semplifica l'applicazione di una configurazione coerente, fornendo al contempo la flessibilità necessaria per modificarla per ogni unità organizzativa e account.

L'account amministratore delegato Security Hub CSPM può anche visualizzare risultati, visualizzare approfondimenti e controllare i dettagli di tutti gli account dei membri. È inoltre possibile designare una regione di aggregazione all'interno dell'account amministratore delegato per centralizzare i

risultati tra i propri account e le regioni collegate. I risultati vengono sincronizzati in modo continuo e bidirezionale tra la regione di aggregazione e tutte le altre regioni.

Security Hub CSPM supporta integrazioni con diversi. Servizi AWS Amazon GuardDuty, Amazon Macie AWS Config, IAM Access Analyzer, Amazon AWS Firewall Manager Inspector, Amazon Route 53 Resolver DNS Firewall e AWS Systems Manager Patch Manager possono inviare i risultati al Security Hub CSPM. Security Hub CSPM elabora i risultati utilizzando un formato standard chiamato AWS Security Finding Format (ASFF). Security Hub CSPM mette in correlazione i risultati tra i prodotti integrati per dare priorità a quelli più importanti. Puoi arricchire i metadati dei risultati CSPM di Security Hub per contribuire a contestualizzare, dare priorità e agire meglio sui risultati di sicurezza. Questo arricchimento aggiunge tag di risorsa, un nuovo tag di AWS applicazione e informazioni sul nome dell'account a ogni risultato che viene inserito in Security Hub CSPM. Ciò consente di ottimizzare i risultati per le regole di automazione, cercare o filtrare risultati e approfondimenti e valutare lo stato del livello di sicurezza per applicazione. Inoltre, puoi utilizzare le regole di automazione per aggiornare automaticamente i risultati. Quando Security Hub CSPM acquisisce i risultati, può applicare una serie di azioni relative alle regole, come sopprimere i risultati, modificarne la gravità e aggiungere note ai risultati. Queste azioni relative alle regole hanno effetto quando i risultati soddisfano i criteri specificati, ad esempio la risorsa o l'account a cui è associato IDs il risultato o il relativo titolo. È possibile utilizzare le regole di automazione per aggiornare alcuni campi di ricerca nell'ASFF. Le regole si applicano sia ai risultati nuovi che a quelli aggiornati.

Durante l'indagine su un evento di sicurezza, puoi passare dal CSPM di Security Hub ad Amazon Detective per indagare su un GuardDuty risultato. Security Hub CSPM consiglia di allineare gli account degli amministratori delegati per servizi come Detective (laddove esistono) per un'integrazione più fluida. Ad esempio, se non allinei gli account amministratore tra Detective e Security Hub CSPM, la navigazione dai risultati a Detective non funzionerà. Per un elenco completo, consulta Panoramica delle Servizio AWS integrazioni con Security Hub CSPM nella documentazione CSPM di Security Hub.

Puoi utilizzare Security Hub CSPM con la funzionalità Network Access Analyzer di Amazon VPC per monitorare continuamente la conformità della configurazione di rete. AWS Questo ti aiuterà a bloccare l'accesso indesiderato alla rete e a impedire l'accesso esterno alle risorse critiche. Per ulteriori dettagli sull'architettura e sull'implementazione, consulta il post AWS sul blog Verifica continua della conformità della rete utilizzando Amazon VPC Network Access Analyzer e. AWS Security Hub CSPM

Oltre alle sue funzionalità di monitoraggio, Security Hub CSPM supporta l'integrazione con Amazon EventBridge per automatizzare la correzione di risultati specifici. È possibile definire

azioni personalizzate da intraprendere quando si riceve un risultato. Ad esempio, puoi configurare operazioni personalizzate per inviare risultati a un sistema di ticket o a un sistema di correzione automatizzato. Per ulteriori discussioni ed esempi, consulta i post del AWS blog Risposta e correzione automatizzate con AWS Security Hub CSPM e Come implementare la AWS soluzione per la risposta e la correzione automatizzate CSPM di Security Hub.

Security Hub CSPM utilizza service-linked Regole di AWS Config per eseguire la maggior parte dei controlli di sicurezza. Per supportare questi controlli, AWS Config deve essere abilitato su tutti gli account, inclusi l'account amministratore (o amministratore delegato) e gli account membro, in tutti gli account in cui è abilitato Security Regione AWS Hub CSPM.

Considerazioni di natura progettuale

- Se uno standard di conformità, come PCI-DSS, è già presente in Security Hub CSPM, il servizio CSPM Security Hub completamente gestito è il modo più semplice per renderlo operativo. Tuttavia, se si desidera creare uno standard di conformità o sicurezza personalizzato, che potrebbe includere controlli di sicurezza, operativi o di ottimizzazione dei costi, i pacchetti di conformità offrono un processo di personalizzazione semplificato. AWS Config (Per ulteriori informazioni sui pacchetti di conformità, AWS Config consulta la sezione.) AWS Config
- I casi d'uso più comuni per Security Hub CSPM includono i seguenti:
  - Come dashboard che offre visibilità ai proprietari delle applicazioni sullo stato di sicurezza e conformità delle loro risorse AWS
  - Come punto di vista centrale dei risultati di sicurezza utilizzati dalle operazioni di sicurezza, dai soccorritori agli incidenti e dai cacciatori di minacce per valutare e intervenire sui risultati di AWS sicurezza e conformità in tutte le regioni Account AWS
  - Per aggregare e indirizzare i risultati di sicurezza e conformità provenienti da diverse regioni, verso un sistema centralizzato di gestione delle informazioni Account AWS e degli eventi di sicurezza (SIEM) o altro sistema di orchestrazione della sicurezza

  Per ulteriori indicazioni su questi casi d'uso, incluso come configurarli, consulta il post sul blog Tre modelli di utilizzo ricorrenti del Security Hub CSPM e come implementarli.

> **Esempio di implementazione**
>
> La libreria di codici AWS SRA fornisce un'implementazione di esempio di Security Hub CSPM. Include l'attivazione automatica del servizio, l'amministrazione delegata a un account membro (Security Tooling) e la configurazione per abilitare Security Hub CSPM per tutti gli account esistenti e futuri dell'organizzazione. AWS

AWS Security Hub

AWS Security Hubè una soluzione di sicurezza cloud unificata che dà priorità alle minacce critiche alla sicurezza e ti aiuta a rispondere su larga scala. Security Hub rileva i problemi di sicurezza quasi in tempo reale correlando e arricchendo automaticamente i segnali di sicurezza provenienti da più fonti, come la gestione della postura (AWS Security Hub CSPM), la gestione delle vulnerabilità (Amazon Inspector), i dati sensibili (Amazon Macie) e il rilevamento delle minacce (Amazon). GuardDuty Ciò consente ai team di sicurezza di dare priorità ai rischi attivi nei loro ambienti cloud attraverso analisi automatizzate e approfondimenti contestuali. Security Hub fornisce una rappresentazione visiva del potenziale percorso di attacco che gli aggressori possono sfruttare per accedere alle risorse associate a un rilevamento dell'esposizione. Questo trasforma segnali di sicurezza complessi in informazioni fruibili, in modo da poter prendere rapidamente decisioni informate sulla sicurezza.

Security Hub è stato riprogettato strategicamente per semplificare l'abilitazione degli elementi costitutivi dei servizi di sicurezza associati per arrivare a un risultato di sicurezza. Correlando i risultati sulla sicurezza in una matrice di minacce tra diversi segnali di sicurezza quasi in tempo reale, puoi dare priorità ai rischi più critici per primi. I risultati sono correlati per rilevare l'esposizione associata alle risorse. AWS Le esposizioni rappresentano punti deboli più ampi nei controlli di sicurezza, configurazioni errate o altre aree che potrebbero essere sfruttate dalle minacce attive. Ad esempio, un'esposizione potrebbe essere un'istanza EC2 raggiungibile da Internet e che presenta vulnerabilità software che hanno un'alta probabilità di sfruttamento.

Security Hub e Security Hub CSPM sono servizi complementari. Security Hub CSPM offre una visione completa del tuo livello di sicurezza e ti aiuta a valutare il tuo ambiente cloud rispetto agli standard e alle best practice del settore della sicurezza. Security Hub offre un'esperienza unificata che ti aiuta a stabilire le priorità e a rispondere ai problemi di sicurezza critici. I risultati CSPM di Security Hub vengono indirizzati automaticamente a Security Hub, dove vengono correlati ai risultati

di altri servizi di sicurezza, come Amazon Inspector, per generare esposizioni. Questo ti aiuta a identificare i rischi più critici nel tuo ambiente.

Security Hub fornisce anche un riepilogo delle risorse presenti nell' AWS ambiente per tipo e risultati associati. Alle risorse viene data priorità in base alle esposizioni e alle sequenze di attacco. Quando scegli un tipo di risorsa, puoi esaminare tutte le risorse associate a quel tipo di risorsa.

Per un'esperienza ottimale, consigliamo di abilitare Security Hub e Security Hub CSPM, oltre a questi altri servizi di sicurezza: Amazon GuardDuty, AmazonInspector e Amazon Macie. Puoi verificare se questi servizi e funzionalità sono abilitati in modo uniforme su tutti gli account membri della tua organizzazione utilizzando i risultati della copertura del Security Hub.

Nell' AWS SRA, l'account Security Tooling funge da amministratore delegato per Security Hub, Security Hub CSPM e altri servizi di sicurezza. AWS All'interno dell'account Security Tooling è possibile visualizzare tutte le risorse associate agli account dei membri. Puoi anche visualizzare tutte le risorse della tua home page Regione AWS da Linked Regioni AWS.

Nota di implementazione

L'attivazione di Security Hub richiede tre passaggi, comprese le procedure che tengono conto dell'eventuale attivazione o meno di Security Hub CSPM in precedenza. Security Hub è integrato nativamente con AWS Organizations, il che semplifica il processo di configurazione e implementazione e centralizza e aggrega tutti i risultati in un'unica posizione. In conformità con le best practice AWS SRA, utilizzate l'account Security Tooling come account amministratore delegato per gestire e configurare Security Hub. Utilizza le impostazioni di configurazione di Security Hub per abilitare automaticamente tutte le regioni e gli account, incluse le regioni e gli account futuri. OUs È inoltre necessario configurare l'aggregazione tra regioni per aggregare risultati, risorse e tendenze provenienti da più regioni Regioni AWS in un'unica area geografica. Durante la configurazione, puoi anche abilitare qualsiasi integrazione nativa come Jira Cloud o. ServiceNow

Considerazioni di natura progettuale

- I risultati di Security Hub sono formattati nell'Open Cybersecurity Schema Framework (OCSF). Security Hub genera risultati in OCSF e riceve risultati in OCSF da Security Hub CSPM e altri. Servizi AWS Questi risultati OCSF possono essere inviati su Amazon

EventBridge per l'automazione o archiviati in un account di aggregazione dei log centrale per eseguire l'analisi e la conservazione dei log di sicurezza.

- L'account AWS Org Management non può designarsi come amministratore delegato in Security Hub. Ciò è in linea con la best practice AWS SRA di designare l'account Security Tooling come amministratore delegato. Nota inoltre:
  - L'account amministratore designato per Security Hub CSPM diventa automaticamente l'amministratore designato per Security Hub.
  - La rimozione dell'amministrazione delegata tramite Security Hub rimuove anche l'amministrazione delegata per Security Hub CSPM. Allo stesso modo, la rimozione dell'amministrazione delegata tramite Security Hub CSPM rimuove anche l'amministrazione delegata per Security Hub.
- Security Hub include funzionalità che modificano e agiscono automaticamente sui risultati in base alle specifiche dell'utente, Security Hub supporta i seguenti tipi di automazioni:
  - Regole di automazione, che aggiornano automaticamente i risultati, li sopprimono e li inviano agli strumenti di ticketing quasi in tempo reale sulla base di criteri definiti.
  - Risposta e correzione automatizzate, che creano EventBridge regole personalizzate che definiscono azioni automatiche da intraprendere in base a risultati e approfondimenti specifici.
- Security Hub può configurare Amazon Inspector in tutti gli account membri e le regioni tramite politiche e può configurare GuardDuty il Security Hub CSPM tramite la distribuzione. Le politiche generano AWS Organizations politiche per account e regioni. Le distribuzioni sono azioni una tantum che abilitano una funzionalità di sicurezza su account e regioni selezionati. Le distribuzioni non si applicano ai nuovi account abilitati. In alternativa, puoi abilitare automaticamente le funzionalità per gli account dei nuovi membri in GuardDuty e Security Hub CSPM.

Amazon GuardDuty

Amazon GuardDuty è un servizio di rilevamento delle minacce che monitora continuamente le attività dannose e i comportamenti non autorizzati per proteggere i tuoi Account AWS carichi di lavoro. Devi sempre acquisire e archiviare i log appropriati per scopi di monitoraggio e controllo, ma GuardDuty estrae flussi di dati indipendenti direttamente dai log di flusso di AWS CloudTrail Amazon VPC e dai log DNS. AWS Non è necessario gestire le policy dei bucket di Amazon S3 o modificare il modo in cui raccogli e archivia i log. GuardDutyle autorizzazioni sono gestite come ruoli collegati ai servizi che

puoi revocare in qualsiasi momento disabilitandoli. GuardDuty Ciò semplifica l'attivazione del servizio senza configurazioni complesse ed elimina il rischio che una modifica delle autorizzazioni IAM o una modifica della policy del bucket S3 influiscano sul funzionamento del servizio.

Oltre a fornire fonti di dati di base, GuardDuty offre funzionalità opzionali per identificare i problemi di sicurezza. Questi includono EKS Protection, RDS Protection, S3 Protection, Malware Protection e Lambda Protection. Per i nuovi rilevatori, queste funzionalità opzionali sono abilitate di default ad eccezione di EKS Protection, che deve essere abilitata manualmente.

- Con GuardDuty S3 Protection, GuardDuty monitora gli eventi relativi ai dati di Amazon S3 oltre CloudTrail agli eventi di gestione predefiniti. CloudTrail Il monitoraggio degli eventi relativi ai dati consente di GuardDuty monitorare le operazioni API a livello di oggetto per individuare potenziali rischi per la sicurezza dei dati all'interno dei bucket S3.
- GuardDuty Malware Protection rileva la presenza di malware sulle istanze Amazon EC2 o sui carichi di lavoro dei container avviando scansioni senza agenti sui volumi Amazon Elastic Block Store (Amazon EBS) collegati. GuardDuty rileva inoltre il potenziale malware nei bucket S3 scansionando gli oggetti appena caricati o le nuove versioni di oggetti esistenti.
- GuardDuty RDS Protection è progettato per profilare e monitorare l'attività di accesso ai database Amazon Aurora senza influire sulle prestazioni del database.
- GuardDuty EKS Protection include EKS Audit Log Monitoring e EKS Runtime Monitoring. Con EKS Audit Log Monitoring, GuardDuty monitora i log di audit Kubernetes dai cluster Amazon EKS e li analizza per attività potenzialmente dannose e sospette. EKS Runtime Monitoring utilizza l'agente di GuardDuty sicurezza (che è un componente aggiuntivo di Amazon EKS) per fornire visibilità di runtime nei singoli carichi di lavoro Amazon EKS. L'agente GuardDuty di sicurezza aiuta a identificare contenitori specifici all'interno dei cluster Amazon EKS che sono potenzialmente compromessi. Può anche rilevare i tentativi di trasferire i privilegi da un singolo container all'host Amazon EC2 sottostante o all'ambiente più ampio. AWS

GuardDuty fornisce inoltre una funzionalità nota come Extended Threat Detection che rileva automaticamente gli attacchi in più fasi che riguardano fonti di dati, più tipi di risorse e un periodo di tempo all'interno di un. AWS Account AWS GuardDutymette in correlazione questi eventi, denominati segnali, per identificare gli scenari che si presentano come potenziali minacce all' AWS ambiente e quindi genera una ricerca della sequenza di attacco. Sono compresi gli scenari di minaccia che comportano compromissioni legate all'uso improprio AWS delle credenziali e tentativi di compromissione dei dati nell'ambiente. Account AWS GuardDuty considera critici tutti i tipi di ricerca

delle sequenze di attacco. Questa funzionalità è abilitata per impostazione predefinita e non comporta costi aggiuntivi.

Nell' AWS SRA, GuardDuty è abilitata in tutti gli account tramite AWS Organizations e tutti i risultati sono visualizzabili e utilizzabili dai team di sicurezza appropriati nell'account amministratore GuardDuty delegato (in questo caso, l'account Security Tooling). GuardDuty i risultati attivi vengono esportati in un bucket S3 centrale nell'account Log Archive, in modo da poterli conservare per più di 90 giorni. I risultati vengono esportati dall'account amministratore delegato e includono anche tutti i risultati degli account dei membri associati nella stessa regione. I risultati nel bucket S3 sono crittografati con una AWS KMS chiave gestita dal cliente. La policy del bucket S3 e la policy delle chiavi KMS sono configurate per consentire solo GuardDuty l'utilizzo delle risorse.

Quando AWS Security Hub CSPM è abilitato, GuardDuty i risultati vengono trasferiti automaticamente a Security Hub CSPM e Security Hub. Quando Amazon Detective è abilitato, GuardDuty i risultati vengono inclusi nel processo di inserimento dei log di Detective. GuardDuty e Detective supportano i flussi di lavoro degli utenti con più servizi, dove GuardDuty fornisce collegamenti dalla console che reindirizzano l'utente da un risultato selezionato a una pagina Detective che contiene un set curato di visualizzazioni per indagare su tale risultato. Ad esempio, puoi anche integrarti GuardDuty con Amazon EventBridge per automatizzare le migliori pratiche GuardDuty, come l'automazione delle risposte a nuove GuardDuty scoperte.

> **Esempio di implementazione**
>
> La libreria di codici AWS SRA fornisce un'implementazione di esempio di GuardDuty. Include la configurazione crittografata del bucket S3, l'amministrazione delegata e l' GuardDuty abilitazione per tutti gli account esistenti e futuri dell'organizzazione. AWS

AWS Config

AWS Configè un servizio che consente di valutare, controllare e valutare le configurazioni delle risorse supportate nel vostro. AWS Account AWS AWS Config monitora e registra continuamente le configurazioni AWS delle risorse e valuta automaticamente le configurazioni registrate rispetto alle configurazioni desiderate. È inoltre possibile integrarsi AWS Config con altri servizi per svolgere il lavoro pesante delle pipeline di audit e monitoraggio automatizzate. Ad esempio, AWS Config può monitorare le modifiche ai singoli segreti in Gestione dei segreti AWS.

È possibile valutare le impostazioni di configurazione AWS delle risorse utilizzando Regole di AWS Config. AWS Config fornisce una libreria di regole predefinite personalizzabili denominate regole gestite oppure è possibile scrivere regole personalizzate. È possibile eseguire Regole di AWS Config in modalità proattiva (prima che le risorse siano state distribuite) o in modalità investigativa (dopo che le risorse sono state distribuite). Le risorse possono essere valutate in caso di modifiche alla configurazione, in base a una pianificazione periodica o in entrambi i casi.

Un pacchetto di conformità è una raccolta di AWS Config regole e azioni correttive che possono essere implementate come singola entità in un account e in una regione o all'interno di un'organizzazione in. AWS Organizations I pacchetti di conformità vengono creati creando un modello YAML che contiene l'elenco di regole gestite o personalizzate e azioni correttive. AWS Config Per iniziare a valutare il tuo AWS ambiente, usa uno dei modelli di pacchetto di conformità di esempio.

AWS Config si integra con AWS Security Hub CSPM per inviare i risultati delle valutazioni AWS Config gestite e personalizzate delle regole come risultati in Security Hub CSPM.

Regole di AWS Config può essere utilizzato insieme a per correggere efficacemente le risorse AWS Systems Manager non conformi. Si utilizza Systems Manager Explorer per raccogliere lo stato di conformità delle AWS Config regole in vigore Regioni AWS e quindi utilizzare i documenti di Systems Manager Automation (runbook) per risolvere le regole non conformi AWS Config . Account AWS Per i dettagli sull'implementazione, consulta il post di blog Rimediare alle regole non AWS Config conformi con i runbook di automazione. AWS Systems Manager

L' AWS Config aggregatore raccoglie dati di configurazione e conformità su più account, regioni e organizzazioni in. AWS Organizations La dashboard dell'aggregatore mostra i dati di configurazione delle risorse aggregate. I dashboard di inventario e conformità offrono informazioni essenziali e aggiornate sulle configurazioni AWS delle risorse e sullo stato di conformità all'interno Account AWS, all'interno o all'interno di un' Regioni AWS organizzazione. AWS Consentono di visualizzare e valutare l'inventario AWS delle risorse senza dover scrivere domande avanzate. AWS Config Puoi ottenere informazioni essenziali come un riepilogo della conformità per risorse, i primi 10 account con risorse non conformi, un confronto tra istanze EC2 in esecuzione e interrotte per tipo e volumi EBS per tipo e dimensione di volume.

Se gestisci la tua AWS organizzazione, questa implementerà una serie di AWS Config regole come barriere investigative (classificate come obbligatorie, fortemente consigliate o facoltative). AWS Control Tower Queste barriere ti aiutano a gestire le tue risorse e a monitorare la conformità tra gli

account della tua organizzazione. AWS Queste AWS Config regole utilizzeranno automaticamente un `aws-control-tower` tag con un valore di. `managed-by-control-tower`

AWS Config deve essere abilitato per ogni account membro dell' AWS organizzazione e Regione AWS deve contenere le risorse che si desidera proteggere. Puoi gestire centralmente (ad esempio, creare, aggiornare ed eliminare) AWS Config le regole per tutti gli account all'interno AWS dell'organizzazione. Dall'account amministratore AWS Config delegato, è possibile implementare un insieme comune di AWS Config regole per tutti gli account e specificare gli account in cui AWS Config le regole non devono essere create. L'account amministratore AWS Config delegato può anche aggregare i dati di configurazione e conformità delle risorse di tutti gli account membri per fornire una vista unica. Utilizza l'account APIs dell'amministratore delegato per applicare la governance assicurandoti che le AWS Config regole sottostanti non possano essere modificate dagli account dei membri dell'organizzazione. AWS AWS Config è integrato nativamente a cui inviare i risultati AWS Security Hub CSPM, se Security Hub CSPM è abilitato ed esiste almeno una regola AWS Config gestita o personalizzata.

In AWS SRA, l'account amministratore AWS Config delegato è l'account Security Tooling. Il canale AWS Config di distribuzione è configurato per fornire istantanee della configurazione delle risorse in un bucket S3 centralizzato nell'account Log Archive. Poiché l'account Log Archive è l'archivio centrale dell'archivio dei log, viene utilizzato per archiviare la configurazione delle risorse.

Considerazioni di natura progettuale

- AWS Config trasmette le notifiche di modifica della configurazione e della conformità ad Amazon EventBridge. Ciò significa che puoi utilizzare le funzionalità di filtro native EventBridge per filtrare AWS Config gli eventi in modo da poter indirizzare tipi specifici di notifiche a obiettivi specifici. Ad esempio, è possibile inviare notifiche di conformità per regole o tipi di risorse specifici a indirizzi e-mail specifici o indirizzare le notifiche di modifica della configurazione a uno strumento esterno di gestione dei servizi IT (ITSM) o di database di gestione della configurazione (CMDB). Per ulteriori informazioni, consulta le AWS Config best practice del post di blog.
- Oltre a utilizzare la valutazione AWS Config proattiva delle regole, è possibile utilizzare AWS CloudFormation Guard, uno strumento di policy-as-code valutazione che verifica in modo proattivo la conformità della configurazione delle risorse. L'interfaccia a riga di AWS CloudFormation Guard comando (CLI) fornisce un linguaggio dichiarativo specifico del dominio (DSL) che è possibile utilizzare per esprimere le politiche sotto forma di codice. Inoltre, puoi utilizzare AWS CLI i comandi per convalidare dati strutturati in formato

JSON o YAML come set di modifiche, file di configurazione Terraform basati su JSON o configurazioni Kubernetes. CloudFormation È possibile eseguire le valutazioni localmente utilizzando la AWS CloudFormation Guard CLI come parte del processo di creazione o eseguirla all'interno della pipeline di distribuzione. Se disponi di AWS Cloud Development Kit (AWS CDK)applicazioni, puoi utilizzare cdk-nag per il controllo proattivo delle migliori pratiche.

Esempio di implementazione

La libreria di codici AWS SRA fornisce un'implementazione di esempio che distribuisce pacchetti di AWS Config conformità a tutte le regioni all'interno di un' Account AWS organizzazione. AWS Il modulo AWS Config Aggregator consente di configurare un AWS Config aggregatore delegando l'amministrazione a un account membro (strumenti di sicurezza) all'interno dell'account di gestione dell'organizzazione e quindi configurando AWS Config Aggregator all'interno dell'account amministratore delegato per tutti gli account esistenti e futuri dell'organizzazione. AWS Puoi utilizzare il modulo AWS Config Control Tower Management Account per abilitarlo AWS Config all'interno dell'account Org Management – non è abilitato da. AWS Control Tower

Amazon Security Lake

Amazon Security Lake è un servizio di data lake di sicurezza completamente gestito. Puoi utilizzare Security Lake per centralizzare automaticamente i dati di sicurezza provenienti da AWS ambienti, fornitori di software as a service (SaaS), locali e fonti di terze parti. Security Lake ti aiuta a creare una fonte di dati normalizzata che semplifica l'uso degli strumenti di analisi rispetto ai dati di sicurezza, in modo da ottenere una comprensione più completa del tuo livello di sicurezza in tutta l'organizzazione. Il data lake è supportato da bucket Amazon Simple Storage Service (Amazon S3) e tu mantieni la proprietà dei tuoi dati. Security Lake raccoglie automaticamente i log per Servizi AWS, tra cui, log di audit, risultati e log AWS Security Hub CSPM di AWS CloudTrail Amazon VPC, Amazon Route 53 AWS Lambda, Amazon S3 e Amazon EKS. AWS WAF

AWS SRA consiglia di utilizzare l'account Log Archive come account amministratore delegato per Security Lake. Per ulteriori informazioni sulla configurazione dell'account amministratore delegato, consulta Amazon Security Lake nella sezione Security OU – Account di archiviazione dei log. I team di sicurezza che desiderano accedere ai dati di Security Lake o hanno bisogno della possibilità di

scrivere log non nativi nei bucket Security Lake utilizzando funzioni personalizzate di estrazione, trasformazione e caricamento (ETL) devono operare all'interno dell'account Security Tooling.

Security Lake può raccogliere log da diversi provider cloud, log da soluzioni di terze parti o altri log personalizzati. Si consiglia di utilizzare l'account Security Tooling per eseguire le funzioni ETL per convertire i log in formato Open Cybersecurity Schema Framework (OCSF) e generare un file in formato Apache Parquet. Security Lake crea il ruolo tra account con le autorizzazioni appropriate per l'account Security Tooling e l'origine personalizzata supportata da funzioni Lambda o AWS Glue crawler, per scrivere dati nei bucket S3 per Security Lake.

L'amministratore di Security Lake deve configurare i team di sicurezza che utilizzano l'account Security Tooling e richiedono l'accesso ai log raccolti da Security Lake come abbonati. Security Lake supporta due tipi di accesso per gli abbonati:

- Accesso ai dati: gli abbonati possono accedere direttamente agli oggetti Amazon S3 per Security Lake. Security Lake gestisce l'infrastruttura e le autorizzazioni. Quando configuri l'account Security Tooling come abbonato all'accesso ai dati di Security Lake, l'account riceve una notifica dei nuovi oggetti nei bucket Security Lake tramite Amazon Simple Queue Service (Amazon SQS) e Security Lake crea le autorizzazioni per accedere a tali nuovi oggetti.
- Accesso tramite query: gli abbonati possono interrogare i dati di origine dalle AWS Lake Formation tabelle del bucket S3 utilizzando servizi come Amazon Athena. L'accesso da più account viene impostato automaticamente per l'accesso alle query utilizzando Lake Formation. Quando si configura l'account Security Tooling come abbonato all'accesso alle query di Security Lake, all'account viene concesso l'accesso in sola lettura ai registri dell'account Security Lake. Quando si utilizza questo tipo di sottoscrittore, Athena AWS Glue e le tabelle vengono condivise dall'account Security Lake Log Archive con l'account Security Tooling tramite (). AWS Resource Access Manager AWS RAM Per abilitare questa funzionalità, è necessario aggiornare le impostazioni di condivisione dei dati tra account alla versione 3.

Per ulteriori informazioni sulla creazione di abbonati, consulta Gestione degli abbonati nella documentazione di Security Lake.

Per le migliori pratiche per l'acquisizione di fonti personalizzate, consulta Raccolta di dati da fonti personalizzate nella documentazione di Security Lake.

Puoi utilizzare Amazon Quick Sight, Amazon OpenSearch Service e Amazon SageMaker per configurare analisi sui dati di sicurezza archiviati in Security Lake.

> **Considerazione di natura progettuale**
>
> Se un team dell'applicazione necessita dell'accesso tramite query ai dati di Security Lake per soddisfare un requisito aziendale, l'amministratore di Security Lake deve configurare l'account dell'applicazione come abbonato.

Amazon Macie

Amazon Macie è un servizio di sicurezza e privacy dei dati completamente gestito che utilizza l'apprendimento automatico e il pattern matching per scoprire e proteggere i tuoi dati sensibili in. AWSÈ necessario identificare il tipo e la classificazione dei dati che il carico di lavoro sta elaborando per garantire l'applicazione dei controlli appropriati. Puoi utilizzare Macie per automatizzare il rilevamento e la segnalazione di dati sensibili in due modi: eseguendo il rilevamento automatico dei dati sensibili e creando ed eseguendo processi di rilevamento di dati sensibili. Con il rilevamento automatico dei dati sensibili, Macie valuta l'inventario dei bucket S3 su base giornaliera e utilizza tecniche di campionamento per identificare e selezionare oggetti S3 rappresentativi dai bucket. Macie recupera e analizza quindi gli oggetti selezionati, ispezionandoli alla ricerca di dati sensibili. I lavori di rilevamento di dati sensibili forniscono un'analisi più approfondita e mirata. Con questa opzione, definisci l'ampiezza e la profondità dell'analisi, inclusi i bucket S3 da analizzare, la profondità di campionamento e i criteri personalizzati che derivano dalle proprietà degli oggetti S3. Se Macie rileva un potenziale problema con la sicurezza o la privacy di un bucket, crea una policy per te. Il rilevamento automatico dei dati è abilitato di default per tutti i nuovi clienti Macie e i clienti Macie esistenti possono abilitarlo con un clic.

Macie è abilitato in tutti gli account tramite. AWS Organizations I responsabili che dispongono delle autorizzazioni appropriate nell'account amministratore delegato (in questo caso, l'account Security Tooling) possono abilitare o sospendere Macie in qualsiasi account, creare processi di rilevamento di dati sensibili per i bucket di proprietà degli account dei membri e visualizzare tutti i risultati delle politiche per tutti gli account membri. I risultati relativi ai dati sensibili possono essere visualizzati solo dall'account che ha creato il processo relativo ai dati sensibili. Per ulteriori informazioni, consulta Gestire più account Macie come organizzazione nella documentazione di Macie.

I risultati di Macie vengono esaminati e AWS Security Hub CSPM analizzati. Macie si integra anche con Amazon EventBridge per facilitare le risposte automatiche ai risultati come avvisi, feed ai sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM) e la riparazione automatica.

Considerazioni di natura progettuale

- Se gli oggetti S3 sono crittografati con una chiave AWS Key Management Service (AWS KMS) gestita da te, puoi aggiungere il ruolo collegato al servizio Macie come utente chiave a quella chiave KMS per consentire a Macie di scansionare i dati.
- Macie è ottimizzato per la scansione di oggetti in Amazon S3. Di conseguenza, qualsiasi tipo di oggetto supportato da MacIE che può essere inserito in Amazon S3 (in modo permanente o temporaneo) può essere scansionato alla ricerca di dati sensibili. Ciò significa che i dati provenienti da altre fonti, ad esempio esportazioni periodiche di snapshot di database Amazon Relational Database Service (Amazon RDS) o Amazon Aurora, tabelle Amazon DynamoDB esportate o file di testo estratti da applicazioni native o di terze parti, possono essere spostati su Amazon S3 e valutati da Macie.

Esempio di implementazione

La libreria di codici AWS SRA fornisce un'implementazione di esempio di Amazon Macie. Include la delega dell'amministrazione a un account membro e la configurazione di Macie all'interno dell'account amministratore delegato per tutti gli account esistenti e futuri dell'organizzazione. AWS Macie è inoltre configurato per inviare i risultati a un bucket S3 centrale crittografato con una chiave gestita dal cliente. AWS KMS

Sistema di analisi degli accessi IAM

Per accelerare il percorso di Cloud AWS adozione e continuare a innovare, è fondamentale mantenere uno stretto controllo sugli accessi dettagliati (autorizzazioni), contenere la proliferazione degli accessi e garantire che le autorizzazioni vengano utilizzate in modo efficace. Un accesso eccessivo e inutilizzato presenta problemi di sicurezza e rende più difficile per le aziende applicare il principio del privilegio minimo. Questo principio è un importante pilastro dell'architettura di sicurezza che implica il continuo dimensionamento corretto delle autorizzazioni IAM per bilanciare i requisiti di sicurezza con i requisiti operativi e di sviluppo delle applicazioni. Questo impegno coinvolge diverse parti interessate, tra cui i team di sicurezza centrale e del Cloud Center of Excellence (CCoE), nonché i team di sviluppo decentralizzati.

AWS Identity and Access Management Access Analyzer fornisce strumenti per impostare in modo efficiente le autorizzazioni granulari, verificare le autorizzazioni previste e perfezionare le autorizzazioni rimuovendo gli accessi non utilizzati per aiutarti a soddisfare gli standard di sicurezza aziendali. Offre visibilità sull'accesso esterno e interno alle risorse e sui risultati degli accessi non utilizzati tramite dashboard e. AWSAWS Security Hub CSPM Inoltre, supporta Amazon EventBridge per flussi di lavoro di notifica e correzione personalizzati basati su eventi.

La funzionalità di analisi degli accessi esterni di IAM Access Analyzer consente di identificare le risorse AWS dell'organizzazione e degli account, come i bucket Amazon S3 o i ruoli IAM, condivisi con un'entità esterna. L' AWS organizzazione o l'account che scegli è nota come zona di fiducia. L'analizzatore utilizza il ragionamento automatico per analizzare tutte le risorse supportate all'interno della zona di fiducia e genera risultati per i responsabili che possono accedere alle risorse dall'esterno della zona di fiducia. Questi risultati aiutano a identificare le risorse condivise con un'entità esterna e consentono di visualizzare in anteprima in che modo la politica influenzi l'accesso pubblico e interaccount alla risorsa prima di distribuire le autorizzazioni per le risorse. Questa funzionalità è disponibile senza costi aggiuntivi.

Allo stesso modo, la funzione di ricerca degli analizzatori di accesso interni di IAM Access Analyzer consente di identificare le risorse AWS dell'organizzazione e gli account condivisi con i responsabili interni all'organizzazione o all'account. Questa analisi supporta il principio del privilegio minimo garantendo che le risorse specificate siano accessibili solo ai responsabili designati all'interno dell'organizzazione. Si tratta di una funzionalità a pagamento che richiede una configurazione esplicita delle risorse da ispezionare. Utilizzate questa funzionalità con prudenza per monitorare risorse sensibili specifiche che, per progettazione, devono essere bloccate anche internamente.

I risultati di IAM Access Analyzer ti aiutano anche a identificare gli accessi non utilizzati concessi nelle tue AWS organizzazioni e nei tuoi account, tra cui:

- Ruoli IAM non utilizzati: ruoli che non hanno alcuna attività di accesso all'interno della finestra di utilizzo specificata.
- Utenti, credenziali e chiavi di accesso IAM non utilizzati: credenziali che appartengono agli utenti IAM e vengono utilizzate per accedere e risorse. Servizi AWS
- Policy e autorizzazioni IAM non utilizzate: autorizzazioni a livello di servizio e a livello di azione che non sono state utilizzate da un ruolo all'interno di una finestra di utilizzo specificata. IAM Access Analyzer utilizza policy basate sull'identità collegate ai ruoli per determinare i servizi e le azioni a cui tali ruoli possono accedere. L'analizzatore fornisce una revisione delle autorizzazioni non utilizzate per tutte le autorizzazioni a livello di servizio.

Puoi utilizzare i risultati generati da IAM Access Analyzer per ottenere visibilità e porre rimedio a qualsiasi accesso non intenzionale o non utilizzato in base alle politiche e agli standard di sicurezza della tua organizzazione. Dopo la correzione, questi risultati vengono contrassegnati come risolti alla successiva esecuzione dell'analizzatore. Se il risultato è intenzionale, puoi contrassegnarlo come archiviato in IAM Access Analyzer e dare priorità ad altri risultati che presentano un rischio maggiore per la sicurezza. Inoltre, puoi impostare regole di archiviazione per archiviare automaticamente risultati specifici. Ad esempio, puoi creare una regola di archiviazione per archiviare automaticamente tutti i risultati per un bucket Amazon S3 specifico a cui concedi regolarmente l'accesso.

In qualità di builder, puoi utilizzare IAM Access Analyzer per eseguire controlli automatici delle policy IAM nelle prime fasi del processo di sviluppo e implementazione (CI/CD) per rispettare gli standard di sicurezza aziendali. Puoi integrare i controlli e le revisioni delle politiche personalizzati di IAM Access Analyzer AWS CloudFormation per automatizzare le revisioni delle politiche come parte delle pipeline del tuo team di sviluppo. CI/CD Questo include:

- Convalida delle policy IAM: IAM Access Analyzer convalida le policy in base alla grammatica e alle best practice delle policy IAM. AWS Puoi visualizzare i risultati dei controlli di convalida delle policy, tra cui avvisi di sicurezza, errori, avvertenze generali e suggerimenti per la tua policy. Attualmente sono disponibili oltre 100 controlli di convalida delle politiche che possono essere automatizzati utilizzando () e. AWS Command Line Interface AWS CLI APIs
- Controlli delle policy personalizzate IAM: i controlli delle policy personalizzati di IAM Access Analyzer convalidano le policy rispetto agli standard di sicurezza specificati. I controlli delle policy personalizzati utilizzano il ragionamento automatico per fornire un livello più elevato di garanzia sulla conformità agli standard di sicurezza aziendali. I tipi di controlli delle policy personalizzati includono:
  - Verifica rispetto a una politica di riferimento: quando modifichi una politica, puoi confrontarla con una politica di riferimento, ad esempio una versione esistente della politica, per verificare se l'aggiornamento concede un nuovo accesso. L'CheckNoNewAccessAPI confronta due policy (una policy aggiornata e una policy di riferimento) per determinare se la policy aggiornata introduce un nuovo accesso rispetto alla policy di riferimento e restituisce una risposta positiva o negativa.
  - Confronta un elenco di azioni IAM: puoi utilizzare l'CheckAccessNotGrantedAPI per assicurarti che una policy non conceda l'accesso a un elenco di azioni critiche definite nel tuo standard di sicurezza. Questa API utilizza una policy e un elenco di un massimo di 100 azioni IAM per verificare se la policy consente almeno una delle azioni e restituisce una risposta positiva o negativa.

I team di sicurezza e altri autori di policy IAM possono utilizzare IAM Access Analyzer per creare policy conformi alla grammatica e agli standard di sicurezza delle policy IAM. La creazione manuale di policy della giusta dimensione può essere soggetta a errori e richiedere molto tempo. La funzionalità di generazione delle policy di IAM Access Analyzer aiuta a creare policy IAM basate sull'attività di accesso del principale. IAM Access Analyzer esamina AWS CloudTrail i log relativi ai servizi supportati e genera un modello di policy che contiene le autorizzazioni utilizzate dal principale nell'intervallo di date specificato. È quindi possibile utilizzare questo modello per creare una policy con autorizzazioni granulari che conceda solo le autorizzazioni necessarie.

- È necessario che il CloudTrail percorso sia abilitato affinché il tuo account generi una politica basata sull'attività di accesso.
- IAM Access Analyzer non identifica l'attività a livello di azione per gli eventi relativi ai dati, come gli eventi relativi ai dati di Amazon S3, nelle policy generate.
- L'`iam:PassRole`azione non viene tracciata CloudTrail e non è inclusa nelle politiche generate.

IAM Access Analyzer viene distribuito nell'account Security Tooling tramite la funzionalità di amministratore delegato in. AWS Organizations L'amministratore delegato dispone delle autorizzazioni per creare e gestire analizzatori con l'organizzazione come zona di fiducia. AWS

> **Considerazione di natura progettuale**
>
> Per ottenere risultati relativi all'account (in cui l'account funge da limite affidabile), crei un analizzatore con ambito account in ogni account membro. Questa operazione può essere eseguita nell'ambito della pipeline degli account. I risultati relativi all'account confluiscono in Security Hub CSPM a livello di account membro. Da lì, passano all'account amministratore delegato CSPM di Security Hub (Security Tooling).

> **Esempi di implementazione**
>
> - La libreria di codici AWS SRA fornisce un'implementazione di esempio di IAM Access Analyzer. Dimostra come configurare un analizzatore a livello di organizzazione all'interno di un account amministratore delegato e un analizzatore a livello di account all'interno di ciascun account.

- Per informazioni su come integrare i controlli delle policy personalizzati nei flussi di lavoro di Builder, consulta il post sul blog Introducing IAM Access Analyzer Custom Policy Checks. AWS

AWS Firewall Manager

AWS Firewall Manageraiuta a proteggere la rete semplificando le attività di amministrazione e manutenzione per AWS WAF i AWS Shield Advanced gruppi AWS Network Firewall di sicurezza Amazon VPC e il firewall DNS su più account Amazon Route 53 Resolver e risorse. Con Firewall Manager, puoi configurare le regole del AWS WAF firewall, le protezioni Shield Advanced, i gruppi di sicurezza Amazon VPC, i firewall Network Firewall e le associazioni dei gruppi di regole DNS Firewall solo una volta. Il servizio applica automaticamente le regole e le protezioni su tutti gli account e le risorse, anche quando vengono aggiunte nuove risorse.

Firewall Manager è particolarmente utile quando si desidera proteggere l'intera AWS organizzazione anziché un numero limitato di account e risorse specifici o se si aggiungono frequentemente nuove risorse da proteggere. Firewall Manager utilizza le policy di sicurezza per consentire di definire una serie di configurazioni, incluse le regole, le protezioni e le azioni pertinenti che devono essere implementate e gli account e le risorse (indicati dai tag) da includere o escludere. È possibile creare configurazioni granulari e flessibili pur rimanendo in grado di estendere il controllo a un numero elevato di account e. VPCs Queste politiche applicano in modo automatico e coerente le regole configurate anche quando vengono creati nuovi account e risorse. Firewall Manager è abilitato in tutti gli AWS Organizations account e la configurazione e la gestione vengono eseguite dai team di sicurezza appropriati nell'account amministratore delegato di Firewall Manager (in questo caso, l'account Security Tooling).

È necessario abilitarlo AWS Config per ogni Regione AWS elemento contenente le risorse che si desidera proteggere. Se non si desidera abilitare AWS Config per tutte le risorse, è necessario abilitarla per le risorse associate al tipo di policy di Firewall Manager che si utilizza. Quando si utilizzano entrambi AWS Security Hub CSPM e Firewall Manager, Firewall Manager invia automaticamente i risultati a Security Hub CSPM. Firewall Manager crea i risultati per le risorse che non sono conformi e per gli attacchi rilevati e li invia a Security Hub CSPM. Quando si imposta una policy di Firewall Manager per AWS WAF, è possibile abilitare centralmente la registrazione sulle liste di controllo degli accessi Web (web ACLs) per tutti gli account interessati e centralizzare i log in un unico account.

Con Firewall Manager puoi avere uno o più amministratori in grado di gestire le risorse firewall della tua organizzazione. Quando si assegnano più amministratori, è possibile applicare condizioni di ambito amministrativo restrittive per definire le risorse (account, regioni OUs, tipi di policy) che ogni amministratore può gestire. Ciò offre la flessibilità necessaria per ricoprire diversi ruoli di amministratore all'interno dell'organizzazione e consente di mantenere il principio dell'accesso con privilegi minimi. L' AWS SRA utilizza un amministratore con ambito amministrativo completo delegato all'account Security Tooling.

> **Considerazione di natura progettuale**
>
> Gli account manager dei singoli account membri dell' AWS organizzazione possono configurare controlli aggiuntivi (come AWS WAF regole e gruppi di sicurezza Amazon VPC) nei servizi gestiti di Firewall Manager in base alle loro esigenze particolari.

> **Esempio di implementazione**
>
> La libreria di codici AWS SRA fornisce un'implementazione di esempio di Firewall Manager. Dimostra l'amministrazione delegata (Security Tooling), implementa un gruppo di sicurezza massimo consentito, configura una politica di gruppo di sicurezza e configura più politiche. AWS WAF

Amazon EventBridge

Amazon EventBridge è un servizio di bus eventi senza server che semplifica la connessione delle applicazioni con dati provenienti da una varietà di fonti. Viene spesso utilizzato nell'automazione della sicurezza. Puoi impostare regole di routing per determinare dove inviare i dati per creare architetture applicative che reagiscano in tempo reale a tutte le tue fonti di dati. Puoi creare un bus di eventi personalizzato per ricevere eventi dalle tue applicazioni personalizzate, oltre a utilizzare il bus di eventi predefinito in ogni account. È possibile creare un bus di eventi nell'account Security Tooling in grado di ricevere eventi specifici di sicurezza da altri account dell'organizzazione. AWS Ad esempio, collegando Amazon GuardDuty e AWS Security Hub CSPM with Regole di AWS Config EventBridge, crei una pipeline flessibile e automatizzata per il routing dei dati di sicurezza, la generazione di avvisi e la gestione delle azioni per risolvere i problemi.

Considerazioni di natura progettuale

- EventBridge è in grado di indirizzare gli eventi verso una serie di destinazioni diverse. Uno schema utile per automatizzare le azioni di sicurezza consiste nel collegare eventi particolari ai singoli AWS Lambda soccorritori, che intraprendono le azioni appropriate. Ad esempio, in determinate circostanze potresti volerlo utilizzare per EventBridge indirizzare i risultati di un bucket S3 pubblico a un risponditore Lambda che corregge la policy del bucket e rimuove le autorizzazioni pubbliche. Questi risponditori possono essere integrati nei playbook e nei runbook investigativi per coordinare le attività di risposta.
- Una best practice per un team addetto alle operazioni di sicurezza di successo consiste nell'integrare il flusso di eventi e risultati relativi alla sicurezza in un sistema di notifica e flusso di lavoro, ad esempio un sistema di ticketing, un sistema o un altro bug/issue sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM). Ciò elimina il flusso di lavoro dalle e-mail e dai report statici e consente di indirizzare, intensificare e gestire eventi o risultati. Le funzionalità di routing flessibili integrate EventBridge sono un potente fattore abilitante per questa integrazione.

Amazon Detective

Amazon Detective supporta la tua strategia di controllo della sicurezza reattivo semplificando l'analisi, l'indagine e l'identificazione rapida della causa principale dei risultati di sicurezza o delle attività sospette per i tuoi analisti di sicurezza. Detective estrae automaticamente eventi basati sul tempo come tentativi di accesso, chiamate API e traffico di rete dai log e dai AWS CloudTrail log di flusso di Amazon VPC. Detective utilizza questi eventi utilizzando flussi di CloudTrail log indipendenti e log di flusso di Amazon VPC. Puoi usare Detective per accedere a un massimo di un anno di dati storici sugli eventi. Detective utilizza l'apprendimento automatico e la visualizzazione per creare una visione unificata e interattiva del comportamento delle risorse e delle interazioni tra di esse nel tempo, chiamata grafico comportamentale. Puoi esplorare il grafico comportamentale per esaminare diverse azioni, come tentativi di accesso falliti o chiamate API sospette.

Detective si integra con Amazon Security Lake per consentire agli analisti della sicurezza di interrogare e recuperare i log archiviati in Security Lake. Puoi utilizzare questa integrazione per ottenere informazioni aggiuntive dai log e dai CloudTrail log di flusso di Amazon VPC archiviati in Security Lake durante le indagini di sicurezza in Detective.

Detective acquisisce anche i risultati rilevati da Amazon GuardDuty, comprese le minacce rilevate da GuardDuty Runtime Monitoring. Quando un account abilita Detective, diventa l'account amministratore per il grafico del comportamento. Prima di provare ad abilitare Detective, assicurati che il tuo account sia registrato GuardDuty da almeno 48 ore. Se non soddisfi questo requisito, non puoi abilitarlo. DetectiveDetective

Altre fonti di dati opzionali per Detective includono i log di audit di Amazon EKS e AWS Security Hub CSPM. L'origine dati dei log di audit di Amazon EKS migliora le informazioni fornite sui seguenti tipi di entità: cluster Amazon EKS, pod Kubernetes, immagini di container e soggetti Kubernetes. La fonte di dati Security Hub fa parte dei risultati di AWS sicurezza, in quanto mette in correlazione i risultati dei diversi prodotti in Security Hub e li inserisce in Detective.

Detective raggruppa automaticamente più risultati correlati a un singolo evento di compromissione della sicurezza in gruppi di ricerca. Gli autori delle minacce in genere eseguono una sequenza di azioni che portano a molteplici risultati di sicurezza distribuiti tra tempo e risorse. Pertanto, i gruppi di ricerca dovrebbero essere il punto di partenza per le indagini che coinvolgono più entità e risultati. Detective fornisce anche riepiloghi dei gruppi di ricerca utilizzando l'intelligenza artificiale generativa che analizza automaticamente i gruppi di ricerca e fornisce approfondimenti in linguaggio naturale per aiutarti ad accelerare le indagini di sicurezza.

Detective si integra con AWS Organizations. L'account Org Management delega un account membro come account amministratore di Detective. In AWS SRA, questo è l'account Security Tooling. L'account amministratore Detective ha la capacità di abilitare automaticamente tutti gli account dei membri correnti dell'organizzazione come account membri di Detective e anche di aggiungere nuovi account membro man mano che vengono aggiunti all' AWS organizzazione. Gli account amministratore Detective hanno anche la possibilità di invitare gli account dei membri che attualmente non risiedono nell' AWS organizzazione, ma si trovano nella stessa regione, a contribuire con i propri dati al grafico del comportamento dell'account principale. Quando un account membro accetta l'invito ed è abilitato, Detective inizia a inserire ed estrarre i dati dell'account membro in quel grafico comportamentale.

> **Considerazione di natura progettuale**
>
> Puoi accedere a Detective trovando i profili dalle AWS Security Hub CSPM console GuardDuty e. Questi collegamenti possono aiutare a semplificare il processo di indagine. Il tuo account deve essere l'account amministrativo sia per Detective che per il servizio da cui

stai effettuando il pivot (GuardDutyo Security Hub CSPM). Se gli account principali sono gli stessi per i servizi, i collegamenti di integrazione funzionano perfettamente.

AWS Audit Manager

AWS Audit Managerti aiuta a controllare continuamente il tuo AWS utilizzo per semplificare la gestione degli audit e della conformità alle normative e agli standard di settore. Consente di passare dalla raccolta, revisione e gestione manuale delle prove a una soluzione che automatizza la raccolta delle prove, fornisce un modo semplice per tracciare la fonte delle prove di audit, consente la collaborazione in team e aiuta a gestire la sicurezza e l'integrità delle prove. Quando è il momento di effettuare un audit, Gestione audit aiuta a gestire le revisioni dei controlli effettuati dalle parti interessate.

Con Audit Manager è possibile eseguire l'audit sulla base di framework predefiniti come il benchmark Center for Internet Security (CIS), il benchmark CIS AWS Foundations, System and Organization Controls 2 (SOC 2) e il Payment Card Industry Data Security Standard (PCI DSS). Inoltre, offre la possibilità di creare framework personalizzati con controlli standard o personalizzati in base ai requisiti specifici per gli audit interni.

Audit Manager raccoglie quattro tipi di prove. Vengono automatizzati tre tipi di prove: prove di verifica della conformità provenienti da AWS Config e AWS Security Hub CSPM, prove di eventi di gestione e prove di configurazione derivanti da chiamate AWS service-to-service API. AWS CloudTrail Per le prove che non possono essere automatizzate, Audit Manager consente di caricare prove manuali.

Per impostazione predefinita, i dati in Audit Manager sono crittografati utilizzando chiavi AWS gestite. L' AWS SRA utilizza una chiave gestita dal cliente per la crittografia per fornire un maggiore controllo sull'accesso logico. È inoltre necessario configurare un bucket S3 nel punto in Regione AWS cui Audit Manager pubblica il rapporto di valutazione. Questi bucket devono essere crittografati con una chiave gestita dal cliente e avere una policy sui bucket configurata per consentire solo agli Audit Manager di pubblicare report.

> **Note**
>
> Audit Manager aiuta a raccogliere prove rilevanti per verificare la conformità a standard e regolamenti di conformità specifici. Tuttavia, non valuta la tua conformità. Pertanto, le prove raccolte tramite Audit Manager potrebbero non includere dettagli sui processi operativi necessari per gli audit. Audit Manager non sostituisce i consulenti legali o gli esperti di

conformità. Ti consigliamo di avvalerti dei servizi di un valutatore terzo certificato per i framework di conformità in base ai quali sei stato valutato.

Le valutazioni di Audit Manager possono essere eseguite su più account nelle AWS organizzazioni. Audit Manager raccoglie e consolida le prove in un account amministratore delegato in. AWS Organizations Questa funzionalità di controllo viene utilizzata principalmente dai team di controllo interno e di conformità e richiede solo l'accesso in lettura a. Account AWS

Considerazioni di natura progettuale

- Audit Manager integra altri servizi AWS di sicurezza come AWS Security Hub CSPM AWS Security Hub, e aiuta AWS Config a implementare un framework di gestione del rischio. Audit Manager offre funzionalità indipendenti di garanzia del rischio, mentre Security Hub CSPM aiuta a supervisionare i rischi e i pacchetti di AWS Config conformità aiutano a gestire i rischi. I professionisti dell'audit che conoscono il modello a tre linee sviluppato dall'Institute of Internal Auditors (IIA) dovrebbero tenere presente che questa combinazione Servizi AWS consente di coprire le tre linee di difesa. Per ulteriori informazioni, consultate la serie di blog suddivisa in due parti sul blog Cloud AWS Operations & Migrations.
- Affinché Audit Manager possa raccogliere le prove CSPM di Security Hub, l'account amministratore delegato per entrambi i servizi deve essere lo stesso. Account AWS Per questo motivo, nell' AWS SRA, l'account Security Tooling è l'amministratore delegato per Audit Manager.

AWS Artifact

AWS Artifactè ospitato all'interno dell'account Security Tooling per separare la funzionalità di gestione degli artefatti di conformità dall'account Org Management. AWS Questa separazione dei compiti è importante perché si consiglia di evitare di utilizzare l'account di gestione dell' AWS organizzazione per le distribuzioni a meno che non sia assolutamente necessario. Invece, trasferisci le distribuzioni agli account dei membri. Poiché la gestione degli artefatti di controllo può essere eseguita da un account membro e la funzione è strettamente allineata con il team di sicurezza e conformità, l'account Security Tooling è designato come account amministratore per. AWS ArtifactÈ possibile utilizzare AWS Artifact i report per scaricare documenti AWS di sicurezza e conformità, come le certificazioni AWS ISO, i report PCI (Payment Card Industry) e i report SOC (System and Organization Controls).

AWS Artifact non supporta la funzionalità di amministrazione delegata. Puoi invece limitare questa funzionalità ai soli ruoli IAM nell'account Security Tooling che riguardano i tuoi team di audit e conformità, in modo che possano scaricare, esaminare e fornire tali report a revisori esterni, se necessario. Puoi inoltre limitare ruoli IAM specifici in modo che abbiano accesso solo a AWS Artifact report specifici tramite le policy IAM. Per esempi di policy IAM, consulta la AWS Artifact documentazione.

> **Considerazione di natura progettuale**
>
> Se scegli di avere un account dedicato Account AWS ai team di audit e conformità, puoi ospitarlo AWS Artifact in un account di controllo di sicurezza, separato dall'account Security Tooling. AWS Artifact i report forniscono prove che dimostrano che un'organizzazione sta seguendo un processo documentato o soddisfa un requisito specifico. Gli elementi degli audit vengono raccolti e archiviati durante l'intero ciclo di vita di sviluppo del sistema e possono essere utilizzati come prove in audit e valutazioni interni o esterni.

AWS KMS

AWS Key Management Service(AWS KMS) consente di creare e gestire chiavi crittografiche e di controllarne l'uso in un'ampia gamma di applicazioni e all'interno di esse. Servizi AWS AWS KMS è un servizio sicuro e resiliente che utilizza moduli di sicurezza hardware per proteggere le chiavi crittografiche. Segue i processi del ciclo di vita standard del settore per i materiali chiave, come l'archiviazione, la rotazione e il controllo dell'accesso alle chiavi. AWS KMS può aiutare a proteggere i dati con chiavi di crittografia e firma e può essere utilizzato sia per la crittografia lato server che per la crittografia lato client tramite Encryption SDK.AWS Per motivi di protezione e flessibilità, AWS KMS supporta tre tipi di chiavi: chiavi gestite dal cliente, chiavi gestite e chiavi di AWS proprietà. AWS Le chiavi gestite dal cliente sono AWS KMS chiavi Account AWS che potete creare, possedere e gestire. AWS le chiavi gestite sono AWS KMS chiavi del tuo account che vengono create, gestite e utilizzate per tuo conto da un Servizio AWS utente integrato con AWS KMS. AWS le chiavi di proprietà sono una raccolta di AWS KMS chiavi Servizio AWS possedute e gestite per essere utilizzate in più lingue Account AWS. Per ulteriori informazioni sull'uso AWS KMS delle chiavi, consulta la AWS KMS documentazione e i dettagli AWS KMS crittografici.

Un'opzione di implementazione consiste nel centralizzare la responsabilità della gestione delle AWS KMS chiavi su un singolo account, delegando al contempo la possibilità di utilizzare le chiavi nell'account dell'applicazione per le risorse dell'applicazione utilizzando una combinazione di politiche

chiave e IAM. Questo approccio è sicuro e semplice da gestire, ma è possibile incontrare ostacoli dovuti ai limiti di AWS KMS throttling, ai limiti dei servizi di account e al sovraccarico del team di sicurezza delle attività operative di gestione delle chiavi. Un'altra opzione di implementazione consiste nell'adottare un modello decentralizzato in cui sia possibile risiedere in più account e consentire AWS KMS ai responsabili dell'infrastruttura e dei carichi di lavoro di un account specifico di gestire le proprie chiavi. Questo modello offre ai team addetti al carico di lavoro maggiore controllo, flessibilità e agilità sull'uso delle chiavi di crittografia. Inoltre, aiuta a evitare i limiti delle API, limita l'ambito di impatto a uno Account AWS solo e semplifica la reportistica, il controllo e altre attività relative alla conformità. In un modello decentralizzato è importante implementare e applicare dei guardrail in modo che le chiavi decentralizzate siano gestite nello stesso modo e l'utilizzo delle chiavi sia verificato in base alle migliori pratiche e politiche consolidate. AWS KMS Per ulteriori informazioni, consulta il white paper Best Practices.AWS Key Management Service AWS SRA consiglia un modello di gestione delle chiavi distribuito in cui AWS KMS le chiavi risiedono localmente all'interno dell'account in cui vengono utilizzate. Si consiglia di evitare di utilizzare una sola chiave in un unico account per tutte le funzioni crittografiche. Le chiavi possono essere create in base ai requisiti di protezione delle funzioni e dei dati e per applicare il principio del privilegio minimo. In alcuni casi, le autorizzazioni di crittografia verrebbero mantenute separate dalle autorizzazioni di decrittografia e gli amministratori gestirebbero le funzioni del ciclo di vita ma non sarebbero in grado di crittografare o decrittografare i dati con le chiavi che gestiscono.

Nell'account Security Tooling, AWS KMS viene utilizzato per gestire la crittografia dei servizi di sicurezza centralizzati come l'organigramma gestito dall'organizzazione. AWS CloudTrail AWS

AWS Private CA

AWS Autorità di certificazione privata(AWS Private CA) è un servizio CA privato gestito che ti aiuta a gestire in modo sicuro il ciclo di vita dei tuoi certificati TLS privati di entità finale per istanze EC2, contenitori, dispositivi IoT e risorse locali. Consente comunicazioni TLS crittografate con le applicazioni in esecuzione. Con AWS Private CA, è possibile creare una gerarchia CA personalizzata (da una CA principale a certificati subordinati CAs a certificati di entità finale) ed emettere certificati con essa per autenticare utenti interni, computer, applicazioni, servizi, server e altri dispositivi e per firmare il codice informatico. I certificati emessi da una CA privata sono considerati affidabili solo all'interno AWS dell'organizzazione, non su Internet.

Un'infrastruttura a chiave pubblica (PKI) o un team di sicurezza possono essere responsabili della gestione di tutta l'infrastruttura PKI. Ciò include la gestione e la creazione della CA privata. Tuttavia, deve esserci una disposizione che consenta ai team addetti al carico di lavoro di soddisfare autonomamente i requisiti dei certificati. L' AWS SRA rappresenta una gerarchia di CA centralizzata

in cui la CA principale è ospitata all'interno dell'account Security Tooling. Ciò consente ai team addetti alla sicurezza di applicare un controllo di sicurezza rigoroso, poiché la CA principale è la base dell'intera PKI. Tuttavia, la creazione di certificati privati dalla CA privata viene delegata ai team di sviluppo delle applicazioni condividendo la CA con un account dell'applicazione utilizzando (). AWS Resource Access Manager AWS RAM AWS RAM gestisce le autorizzazioni necessarie per la condivisione tra account. Ciò elimina la necessità di una CA privata in ogni account e fornisce un modo di implementazione più conveniente. Per ulteriori informazioni sul flusso di lavoro e sull'implementazione, consulta il post del blog How to use AWS RAM to share your AWS Private CA cross-account.

> **Note**
>
> AWS Certificate Manager (ACM) consente inoltre di fornire, gestire e distribuire certificati TLS pubblici da utilizzare con. Servizi AWS Per supportare questa funzionalità, ACM deve risiedere nel sito Account AWS che utilizzerebbe il certificato pubblico. Questo è discusso più avanti in questa guida, nella sezione Account dell'applicazione.

> **Considerazioni di natura progettuale**
>
> - Con AWS Private CA, è possibile creare una gerarchia di autorità di certificazione con un massimo di cinque livelli. È inoltre possibile creare più gerarchie, ognuna con una propria root. La AWS Private CA gerarchia deve aderire al design PKI dell'organizzazione. Tuttavia, tenete presente che l'aumento della gerarchia CA aumenta il numero di certificati nel percorso di certificazione, il che, a sua volta, aumenta il tempo di convalida di un certificato di entità finale. Una gerarchia CA ben definita offre vantaggi che includono il controllo di sicurezza granulare appropriato per ogni CA, la delega della CA subordinata a un'applicazione diversa, che porta alla divisione delle attività amministrative, l'uso di CA con fiducia revocabile limitata, la capacità di definire periodi di validità diversi e la capacità di applicare limiti di percorso. Idealmente, root e subordinato sono separati. CAs Account AWS Per ulteriori informazioni sulla pianificazione di una gerarchia di CA utilizzando AWS Private CA, consulta la AWS Private CA documentazione e il post di blog Come proteggere una AWS Private CA gerarchia su scala aziendale per il settore automobilistico e manifatturiero.
> - AWS Private CA può integrarsi con la gerarchia CA esistente, il che consente di utilizzare le funzionalità di automazione e AWS integrazione nativa di ACM insieme all'attuale root

of trust. È possibile creare una CA subordinata AWS Private CA supportata da una CA principale in locale. Per ulteriori informazioni sull'implementazione, vedere Installazione di un certificato CA subordinato firmato da una CA principale esterna nella AWS Private CA documentazione.

Amazon Inspector

Amazon Inspector è un servizio automatizzato di gestione delle vulnerabilità che rileva e analizza automaticamente le istanze Amazon EC2, le immagini dei container in Amazon Elastic Container Registry (Amazon ECR), le funzioni e gli archivi di codice all'interno dei gestori del codice sorgente AWS Lambda per individuare vulnerabilità software note ed esposizione involontaria alla rete.

Amazon Inspector valuta continuamente il tuo ambiente durante l'intero ciclo di vita delle tue risorse scansionando automaticamente le risorse ogni volta che apporti modifiche. Gli eventi che avviano la nuova scansione di una risorsa includono l'installazione di un nuovo pacchetto su un'istanza EC2, l'installazione di una patch e la pubblicazione di un nuovo rapporto CVE (Common Vulnerabilities and Exposures) che influisce sulla risorsa. Amazon Inspector supporta le valutazioni benchmark del Center of Internet Security (CIS) per i sistemi operativi nelle istanze EC2.

Amazon Inspector si integra con strumenti di sviluppo come Jenkins e TeamCity per la valutazione delle immagini dei container. Puoi valutare le immagini dei container per individuare eventuali vulnerabilità del software all'interno del pannello di controllo CI/CD) tools, and push security to an earlier point in the software development lifecycle. Assessment findings are available in the CI/CD dello strumento di integrazione continua e distribuzione continua, in modo da eseguire azioni automatizzate in risposta a problemi di sicurezza critici come build bloccate o invio di immagini ai registri dei container. Se ne hai uno attivo Account AWS, puoi installare il plug-in Amazon Inspector dal marketplace CI/CD degli strumenti e aggiungere una scansione Amazon Inspector nella tua pipeline di compilazione senza dover attivare il servizio Amazon Inspector. Questa funzionalità è compatibile con CI/CD strumenti ospitati ovunque, in locale o in cloud ibridi AWS, in modo da poter utilizzare in modo coerente un'unica soluzione in tutte le pipeline di sviluppo. Quando Amazon Inspector è attivato, rileva automaticamente tutte le istanze EC2, le immagini dei container in Amazon ECR e gli strumenti CI/CD e le funzioni Lambda su larga scala e le monitora continuamente per individuare vulnerabilità note.

I risultati sulla raggiungibilità della rete di Amazon Inspector valutano l'accessibilità delle istanze EC2 da o verso i edge VPC come gateway Internet, connessioni peering VPC o reti private virtuali () attraverso un gateway virtuale. VPNs Queste regole aiutano ad automatizzare il monitoraggio delle

AWS reti e a identificare i punti in cui l'accesso di rete alle istanze EC2 potrebbe essere configurato in modo errato a causa di gruppi di sicurezza, elenchi di controllo degli accessi (), gateway Internet e così via. ACLs Per ulteriori informazioni, consulta la documentazione di Amazon Inspector.

Quando Amazon Inspector identifica vulnerabilità o percorsi di rete aperti, produce un risultato che puoi esaminare. La scoperta include dettagli completi sulla vulnerabilità, tra cui un punteggio di rischio, la risorsa interessata e raccomandazioni per la correzione. Il punteggio di rischio è specificamente adattato all'ambiente in uso e viene calcolato correlando le informazioni up-to-date CVE con fattori temporali e ambientali, come l'accessibilità della rete e le informazioni sulla sfruttabilità, per fornire un risultato contestuale.

Amazon Inspector Code Security analizza il codice sorgente delle applicazioni proprietarie, le dipendenze delle applicazioni di terze parti e l'infrastruttura come codice (IaC) alla ricerca di vulnerabilità. Dopo aver attivato Code Security, puoi creare e applicare una configurazione di scansione al tuo repository di codice per determinare la frequenza, il tipo di scansione e gli archivi da scansionare. Code Security supporta i test statici di sicurezza delle applicazioni (SAST), l'analisi della composizione del software (SCA) e la scansione IaC. Per configurare la frequenza, è possibile definire scansioni su richiesta, in caso di modifiche al codice o periodicamente. La scansione del codice acquisisce frammenti di codice per evidenziare le vulnerabilità rilevate. I frammenti di codice vengono archiviati crittografati con chiavi KMS. L'amministratore delegato di un'organizzazione non può visualizzare frammenti di codice che appartengono agli account dei membri. Dopo aver integrato i gestori del codice sorgente (SCMs) con Code Security, tutti gli archivi di codice vengono elencati come progetti nella console Amazon Inspector. Code Security monitora solo il ramo predefinito di ogni repository. Amazon Inspector semplifica la correzione della sicurezza fornendo consigli specifici per la correzione del codice direttamente dove lavorano gli sviluppatori. L'integrazione bidirezionale con SCM suggerisce automaticamente le correzioni sotto forma di commenti nelle richieste pull (PRs) e nelle richieste di unione () in caso di risultati critici e importanti e avvisa gli sviluppatori delle vulnerabilità più importanti da risolvere senza interrompere il flusso di lavoro. MRs

Per individuare le vulnerabilità, le istanze EC2 devono essere gestite utilizzando Agent (SSMAgent). AWS Systems Manager AWS Systems Manager Non sono necessari agenti per la raggiungibilità della rete delle istanze EC2 o la scansione delle vulnerabilità delle immagini dei container nelle funzioni Amazon ECR o Lambda.

Amazon Inspector è integrato AWS Organizations e supporta l'amministrazione delegata. Nell' AWS SRA, l'account Security Tooling diventa l'account amministratore delegato per Amazon Inspector. L'account amministratore delegato di Amazon Inspector può gestire i risultati, i dati e determinate impostazioni per i membri dell'organizzazione. AWS Ciò include la visualizzazione dei dettagli dei

risultati aggregati per tutti gli account dei membri, l'attivazione o la disabilitazione delle scansioni per gli account dei membri e la revisione delle risorse scansionate all'interno dell'organizzazione. AWS

Considerazioni di natura progettuale

- Amazon Inspector si integra automaticamente con Security AWS Security Hub CSPM Hub quando entrambi i servizi sono abilitati. Puoi utilizzare questa integrazione per inviare tutti i risultati da Amazon Inspector a Security Hub CSPM, che li includerà quindi nell'analisi del tuo livello di sicurezza.
- Amazon Inspector esporta automaticamente gli eventi relativi a risultati, modifiche alla copertura delle risorse e scansioni iniziali di singole risorse su Amazon e EventBridge, facoltativamente, in un bucket Amazon Simple Storage Service (Amazon S3). Per esportare i risultati attivi in un bucket S3, è necessaria una AWS KMS chiave che Amazon Inspector possa utilizzare per crittografare i risultati e un bucket S3 con autorizzazioni che consentano ad Amazon Inspector di caricare oggetti. EventBridgel'integrazione ti consente di monitorare ed elaborare i risultati quasi in tempo reale come parte dei flussi di lavoro di sicurezza e conformità esistenti. EventBridge gli eventi vengono pubblicati sull'account amministratore delegato di Amazon Inspector oltre all'account membro da cui hanno avuto origine.
- Le integrazioni di Amazon Inspector Code Security con GitHub SaaS, GitHub Enterprise Cloud ed GitHub Enterprise Server richiedono l'accesso pubblico a Internet.

Esempio di implementazione

La libreria di codici AWS SRA fornisce un'implementazione di esempio di Amazon Inspector. Dimostra l'amministrazione delegata (Security Tooling) e configura Amazon Inspector per tutti gli account esistenti e futuri dell'organizzazione. AWS

AWS Security Incident Response

AWS Security Incident Responseè un servizio che ti aiuta a prepararti e a rispondere agli incidenti di sicurezza nel tuo ambiente. AWS Esamina i risultati, analizza gli eventi di sicurezza e gestisce i casi che richiedono l'attenzione immediata dell'utente. Inoltre, ti dà accesso al AWS Customer Incident Response Team (CIRT), che indaga sulle risorse interessate. AWS Security Incident

Response fornisce inoltre funzionalità automatizzate di risposta e riparazione tramite AWS Systems Manager documenti (documenti SSM), che aiutano i team di sicurezza a rispondere e riprendersi dagli incidenti di sicurezza in modo più efficiente. AWS Security Incident Response si integra con Amazon GuardDuty AWS Security Hub CSPM per ricevere risultati di sicurezza e orchestrare risposte automatiche.

Nell' AWS SRA, AWS Security Incident Response viene distribuito nell'account Security Tooling come account amministratore delegato. L'account Security Tooling è selezionato perché è in linea con lo scopo dell'account di gestire i servizi di sicurezza e automatizzare gli avvisi e le risposte di sicurezza. L'account Security Tooling funge anche da account amministratore delegato per Security Hub CSPM e GuardDuty, insieme AWS Security Incident Response, aiuta a semplificare la gestione del flusso di lavoro. AWS Security Incident Response è configurato per funzionare con AWS Organizations, in modo da poter gestire le risposte agli incidenti tra gli account dell'organizzazione dall'account Security Tooling.

AWS Security Incident Response ti aiuta a implementare le seguenti fasi del ciclo di vita della risposta agli incidenti:

- Preparazione: crea e gestisci piani di risposta e documenti SSM per le azioni di contenimento.
- Rilevamento e analisi: analizza automaticamente i risultati di sicurezza e determina la gravità degli incidenti.
- Rilevamento e analisi: aprite un caso supportato dal servizio e contattate il AWS CIRT per ulteriore assistenza. CIRT è un gruppo di individui che forniscono supporto durante eventi di sicurezza attivi.
- Contenimento ed eradicazione: esegui azioni di contenimento automatizzate tramite documenti SSM.
- Attività post-incidente: documenta i dettagli dell'incidente ed esegui analisi post-incidente.

Puoi anche utilizzarlo AWS Security Incident Response per creare casi autogestiti. AWS Security Incident Response puoi creare una notifica o un caso in uscita quando devi essere a conoscenza di qualcosa che potrebbe influire sul tuo account o sulle tue risorse o agire di conseguenza. Questa funzionalità è disponibile solo quando abiliti i flussi di lavoro di risposta proattiva e triaging degli avvisi come parte dell'abbonamento.

Considerazioni di natura progettuale

- Quando implementi AWS Security Incident Response, esamina e testa attentamente le azioni di risposta automatiche prima di attivarle in produzione. L'automazione può accelerare la risposta agli incidenti, ma le azioni automatizzate configurate in modo errato potrebbero influire sui carichi di lavoro legittimi.
- Prendi in considerazione l'utilizzo di documenti SSM AWS Security Incident Response per implementare procedure di contenimento specifiche dell'organizzazione, mantenendo al contempo le migliori pratiche integrate nel servizio per i tipi di incidenti più comuni.
- Se prevedi di utilizzarlo AWS Security Incident Response in un VPC, assicurati di avere gli endpoint VPC appropriati configurati per Systems Manager e altri servizi integrati per abilitare le azioni di contenimento nelle sottoreti private.

Implementazione di servizi di sicurezza comuni all'interno di tutti Account AWS

La sezione Applica i servizi di sicurezza all'intera AWS organizzazione precedente di questo riferimento ha evidenziato i servizi di sicurezza che proteggono un Account AWS utente e ha osservato che molti di questi servizi possono essere configurati e gestiti anche all'interno AWS Organizations. Alcuni di questi servizi devono essere distribuiti in tutti gli account e li vedrai nell' AWS SRA. Ciò consente una serie coerente di barriere e fornisce monitoraggio, gestione e governance centralizzati in tutta l'organizzazione. AWS

Security Hub, CSPM, GuardDuty AWS Config, IAM Access Analyzer e gli itinerari CloudTrail dell'organizzazione vengono visualizzati in tutti gli account. I primi tre supportano la funzionalità di amministratore delegato descritta in precedenza nella sezione Account di gestione, accesso affidabile e amministratori delegati. CloudTrail attualmente utilizza un meccanismo di aggregazione diverso.

L'archivio del GitHub codice AWS SRA fornisce un'implementazione di esempio per abilitare Security Hub, CSPM, GuardDuty AWS Config AWS Firewall Manager, e i percorsi CloudTrail organizzativi su tutti gli account, incluso l' AWS account Org Management.

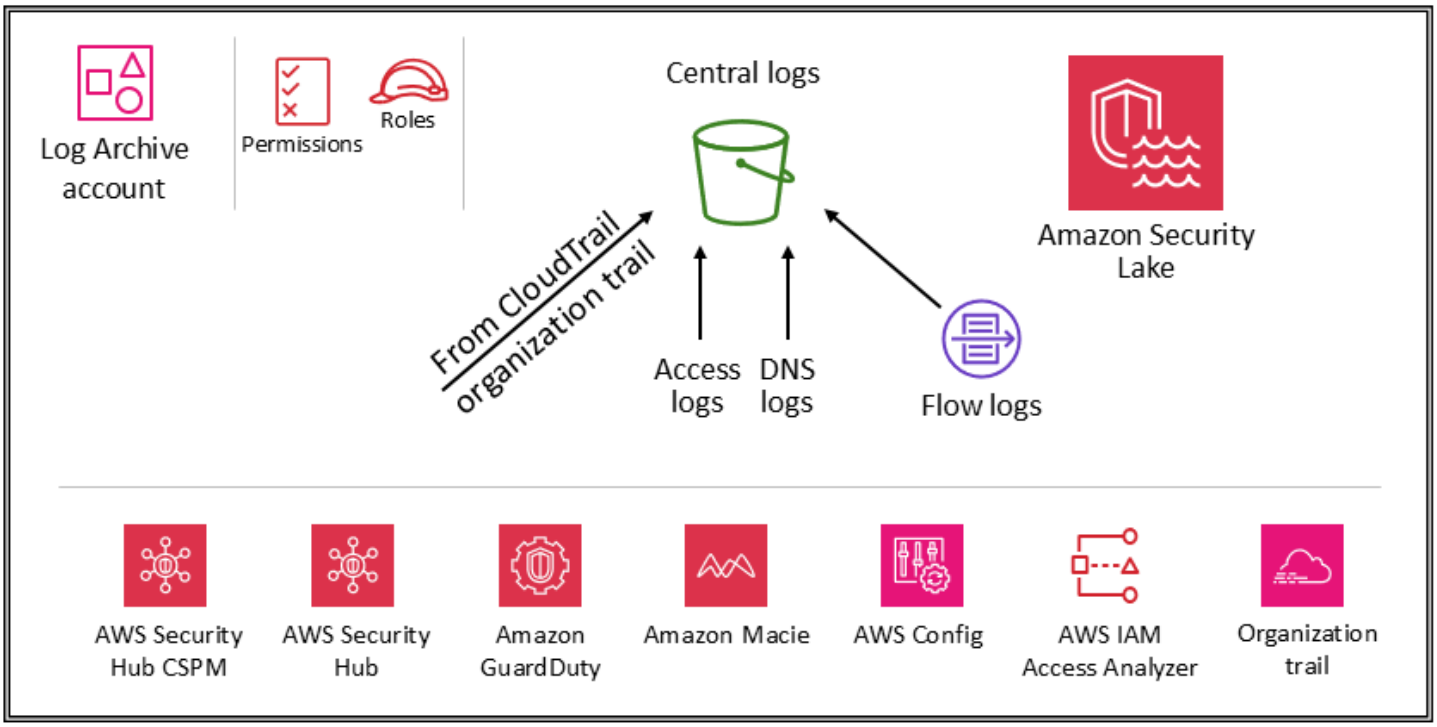
Considerazioni di natura progettuale

- Le configurazioni specifiche degli account potrebbero richiedere servizi di sicurezza aggiuntivi. Ad esempio, gli account che gestiscono i bucket S3 (gli account Application e Log Archive) dovrebbero includere anche Amazon Macie e prendere in considerazione l'attivazione della registrazione degli eventi dei dati S3 CloudTrail in questi servizi di sicurezza comuni. (Macie supporta l'amministrazione delegata con configurazione e monitoraggio centralizzati.) Un altro esempio è Amazon Inspector, applicabile solo agli account che ospitano istanze EC2 o immagini Amazon ECR.
- Oltre ai servizi descritti in precedenza in questa sezione, l' AWS SRA include due servizi incentrati sulla sicurezza, Amazon Detective e AWS Audit Manager, che supportano AWS Organizations l'integrazione e la funzionalità di amministratore delegato. Tuttavia, questi servizi non sono inclusi tra i servizi consigliati per la baselining degli account, poiché abbiamo visto che questi servizi vengono utilizzati al meglio nei seguenti scenari:
  - Hai un team o un gruppo di risorse dedicato che svolgono queste funzioni. Detective viene utilizzato al meglio dai team di analisti della sicurezza e Audit Manager è utile per i team interni di audit o conformità.
  - Desideri concentrarti su un set di strumenti di base come GuardDuty Security Hub CSPM all'inizio del progetto e poi sfruttarli utilizzando servizi che forniscono funzionalità aggiuntive.

Unità organizzativa di sicurezza — Account Log Archive

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

Il diagramma seguente illustra i servizi AWS di sicurezza configurati nell'account Log Archive.



L'account Log Archive è dedicato all'acquisizione e all'archiviazione di tutti i log e i backup relativi alla sicurezza. Con i log centralizzati, puoi monitorare, controllare e inviare avvisi sull'accesso agli oggetti di Amazon S3, sulle attività non autorizzate delle identità, sulle modifiche alle policy IAM e su altre attività critiche eseguite su risorse sensibili. Gli obiettivi di sicurezza sono semplici: deve trattarsi di uno storage immutabile, accessibile solo da meccanismi controllati, automatizzati e monitorati e progettato per garantire la durabilità (ad esempio, utilizzando i processi di replica e archiviazione appropriati). I controlli possono essere implementati in profondità per proteggere l'integrità e la disponibilità dei log e del processo di gestione dei log. Oltre ai controlli preventivi, come l'assegnazione di ruoli con privilegi minimi da utilizzare per l'accesso e la crittografia dei log con una AWS KMS chiave controllata, utilizza controlli di rilevamento come monitorare (e avvisare e correggere) questa raccolta di autorizzazioni AWS Config per modifiche impreviste.

> **Considerazione di natura progettuale**
>
> I dati di registro operativi utilizzati dai team di infrastruttura, operazioni e carico di lavoro spesso si sovrappongono ai dati di registro utilizzati dai team di sicurezza, audit e conformità. Ti consigliamo di consolidare i dati di registro operativi nell'account Log Archive. In base ai requisiti specifici di sicurezza e governance, potrebbe essere necessario filtrare i dati di registro operativi salvati su questo account. Potrebbe inoltre essere necessario specificare chi ha accesso ai dati di registro operativi nell'account Log Archive.

Tipi di log

I log principali mostrati nell' AWS SRA includono AWS CloudTrail (percorso organizzativo), log di flusso di Amazon VPC, log di accesso di Amazon CloudFront AWS WAF e log DNS di Amazon Route 53. Questi log forniscono un controllo delle azioni intraprese (o tentate) da un utente, un ruolo o un'entità di rete (identificata Servizio AWS, ad esempio, da un indirizzo IP). È possibile acquisire e archiviare anche altri tipi di registro (ad esempio registri delle applicazioni o dei database). Per ulteriori informazioni sulle fonti di registro e sulle migliori pratiche di registrazione, consulta la documentazione sulla sicurezza di ciascun servizio.

Amazon S3 come archivio di log centrale

Molte informazioni di Servizi AWS log in Amazon S3, di default o esclusivamente. AWS CloudTrail, Amazon VPC Flow Logs, Elastic Load Balancing AWS Config, GuardDuty Amazon AWS WAF e sono alcuni esempi di servizi che registrano informazioni in Amazon S3. Ciò significa che l'integrità dei log viene raggiunta attraverso l'integrità degli oggetti S3, la riservatezza dei log viene ottenuta tramite i controlli di accesso agli oggetti S3 e la disponibilità dei log viene ottenuta tramite S3 Object Lock, le versioni degli oggetti S3 e le regole S3 Lifecycle. Registrando le informazioni in un bucket S3 dedicato e centralizzato che risiede in un account dedicato, puoi gestire questi log in pochi bucket e applicare rigorosi controlli di sicurezza, accesso e separazione delle funzioni.

Nell' AWS SRA, provengono CloudTrail i log primari archiviati in Amazon S3, quindi questa sezione descrive come proteggere tali oggetti. Questa guida si applica anche a qualsiasi altro oggetto S3 creato dalle tue applicazioni o da altri. Servizi AWS Applica questi modelli ogni volta che hai dati in Amazon S3 che richiedono elevata integrità, forte controllo degli accessi e conservazione o distruzione automatizzate.

Tutti i nuovi oggetti (compresi CloudTrail i log) caricati nei bucket S3 sono crittografati per impostazione predefinita utilizzando la crittografia lato server di Amazon con chiavi di crittografia gestite da Amazon S3 (SSE-S3). Ciò aiuta a proteggere i dati archiviati, ma il controllo degli accessi è controllato esclusivamente dalle politiche IAM. Per fornire un ulteriore livello di sicurezza gestito, puoi utilizzare la crittografia lato server con AWS KMS chiavi gestite dall'utente (SSE-KMS) su tutti i bucket di sicurezza S3. Ciò aggiunge un secondo livello di controllo degli accessi. Per leggere i file di log, un utente deve disporre sia delle autorizzazioni di lettura di Amazon S3 per l'oggetto S3 sia di una policy o di un ruolo IAM applicato che consenta loro le autorizzazioni di decrittografia in base alla policy chiave associata.

Due opzioni consentono di proteggere o verificare l'integrità degli oggetti di CloudTrail log archiviati in Amazon S3. CloudTrail fornisce la convalida dell'integrità dei file di registro per determinare se un file di registro è stato modificato o eliminato dopo la CloudTrail consegna. L'altra opzione è S3 Object Lock.

Oltre a proteggere il bucket S3 stesso, puoi rispettare il principio del privilegio minimo per i servizi di registrazione (ad esempio CloudTrail) e l'account Log Archive. Ad esempio, gli utenti con le autorizzazioni concesse dalla policy IAM AWS gestita `AWSCloudTrail_FullAccess` possono disabilitare o riconfigurare le funzioni di controllo più sensibili e importanti al loro interno. Account AWS Limita l'applicazione di questa policy IAM al minor numero possibile di individui.

Utilizza i controlli investigativi, come quelli forniti da AWS Config IAM Access Analyzer, per monitorare (e avvisare e porre rimedio) a questo più ampio collettivo di controlli preventivi in caso di modifiche impreviste.

Per una discussione più approfondita sulle best practice di sicurezza per i bucket S3, consulta la documentazione di Amazon S3, i talk tecnici online e il post sul blog Le 10 migliori pratiche di sicurezza per la protezione dei dati in Amazon S3.

> **Esempio di implementazione**
>
> La libreria di codici AWS SRA fornisce un'implementazione di esempio dell'accesso pubblico tramite account a blocchi Amazon S3. Questo modulo blocca l'accesso pubblico ad Amazon S3 per tutti gli account esistenti e futuri dell' AWS organizzazione.

Amazon Security Lake

AWS SRA consiglia di utilizzare l'account Log Archive come account amministratore delegato per Amazon Security Lake. In tal caso, Security Lake raccoglie i log supportati in bucket S3 dedicati nello stesso account degli altri log di sicurezza consigliati da SRA.

Per proteggere la disponibilità dei log e il processo di gestione dei log, è necessario accedere ai bucket S3 per Security Lake solo dal servizio Security Lake o dai ruoli IAM gestiti da Security Lake per sorgenti o abbonati. Oltre a utilizzare controlli preventivi, come l'assegnazione di ruoli con privilegi minimi per l'accesso e la crittografia dei log con una AWS KMS chiave controllata, utilizza controlli investigativi come AWS Config monitorare (e avvisare e correggere) questa raccolta di autorizzazioni per modifiche impreviste.

L'amministratore di Security Lake AWS può abilitare la raccolta dei log in tutta l'organizzazione. Questi registri sono archiviati in bucket S3 regionali nell'account Log Archive. Inoltre, per centralizzare i log e facilitare l'archiviazione e l'analisi, l'amministratore di Security Lake può scegliere una o più regioni di rollup in cui i log di tutti i bucket S3 regionali vengono consolidati e archiviati. I log di Supported Servizi AWS vengono convertiti automaticamente in uno schema open source standardizzato chiamato Open Cybersecurity Schema Framework (OCSF) e salvati in formato Apache Parquet nei bucket Security Lake S3. Con il supporto OCSF, Security Lake normalizza e consolida in modo efficiente i dati di sicurezza provenienti e da altre fonti di sicurezza aziendali per creare un archivio unificato AWS e affidabile di informazioni relative alla sicurezza.

Security Lake può raccogliere log associati a eventi di AWS CloudTrail gestione ed eventi relativi ai CloudTrail dati per Amazon AWS Lambda S3 e. Per raccogliere eventi di CloudTrail gestione in Security Lake, è necessario disporre di almeno un percorso organizzativo CloudTrail multiregionale che raccolga gli eventi di gestione di lettura e scrittura. CloudTrail La registrazione deve essere abilitata per il percorso. Un percorso multiregionale fornisce file di registro da più regioni a un singolo bucket S3 per uno. Account AWS Se le regioni si trovano in paesi diversi, considera i requisiti di esportazione dei dati per determinare se è possibile abilitare percorsi multiregionali.

AWS Security Hub CSPM è un'origine dati nativa supportata in Security Lake ed è necessario aggiungere i risultati CSPM di Security Hub a Security Lake. Security Hub CSPM genera risultati da molte integrazioni diverse Servizi AWS e di terze parti. Questi risultati ti aiutano a ottenere una panoramica del tuo atteggiamento di conformità e a verificare se stai seguendo le raccomandazioni e le soluzioni di sicurezza. AWS AWS Partner

Per ottenere visibilità e informazioni utili da log ed eventi, puoi interrogare i dati utilizzando strumenti come Amazon Athena, Amazon Service OpenSearch , Amazon Quick e soluzioni di terze parti. Gli utenti che richiedono l'accesso ai dati di registro di Security Lake non devono accedere direttamente all'account Log Archive. Devono accedere ai dati solo dall'account Security Tooling. Oppure possono utilizzare altre sedi Account AWS o locali che forniscono strumenti di analisi come OpenSearch Service, Quick o strumenti di terze parti come gli strumenti di gestione delle informazioni e degli eventi di sicurezza (SIEM). Per fornire l'accesso ai dati, l'amministratore deve configurare gli abbonati a Security Lake nell'account Log Archive e configurare l'account che richiede l'accesso ai dati come abbonato all'accesso alle query. Per ulteriori informazioni, consulta Amazon Security Lake nella sezione Security OU – Security Tooling account di questa guida.

Security Lake fornisce una policy AWS gestita per aiutarti a gestire l'accesso degli amministratori al servizio. Per ulteriori informazioni, consulta la Guida per l'utente di Security Lake. Come procedura ottimale, si consiglia di limitare la configurazione di Security Lake tramite pipeline di sviluppo e

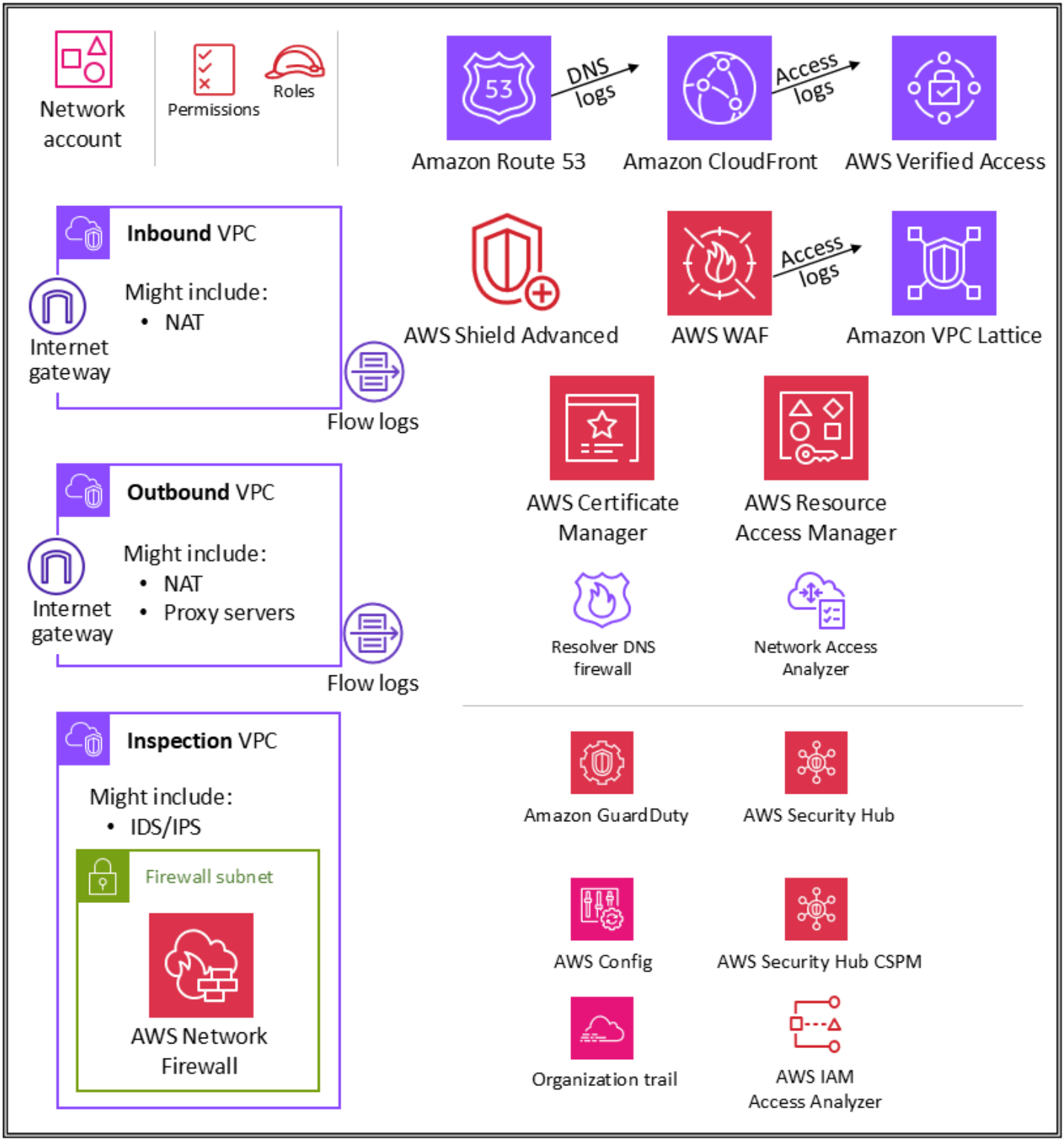
impedire modifiche alla configurazione tramite AWS le console o il AWS Command Line Interface ()AWS CLI. Inoltre, è necessario impostare politiche IAM e politiche di controllo del servizio rigorose (SCPs) per fornire solo le autorizzazioni necessarie per gestire Security Lake. Puoi configurare le notifiche per rilevare qualsiasi accesso diretto a questi bucket S3.

> **Considerazione di natura progettuale**
>
> Quando si abilitano gli eventi di CloudTrail gestione in Security Lake, questi comportano addebiti per Security Lake. La raccolta di eventi di CloudTrail gestione in Security Lake richiede un percorso organizzativo CloudTrail multiregionale che raccolga gli eventi di CloudTrail gestione di lettura e scrittura. Questo primo percorso è disponibile gratuitamente. CloudTrail gli eventi di gestione rappresentano in genere una piccola percentuale (circa il 5%) degli CloudTrail eventi totali. Questo vale per i clienti che utilizzano AWS Control Tower o dispongono di CloudTrail log centralizzati in un account Log Archive.

UO dell'infrastruttura - Account di rete

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

Il diagramma seguente illustra i servizi AWS di sicurezza configurati nell'account di rete.



L'account di rete gestisce il gateway tra l'applicazione e Internet in generale. È importante proteggere quell'interfaccia bidirezionale. L'account di rete isola i servizi di rete, la configurazione e il funzionamento dai carichi di lavoro, dalla sicurezza e da altre infrastrutture delle singole applicazioni.

Questa disposizione non solo limita la connettività, le autorizzazioni e il flusso di dati, ma supporta anche la separazione dei compiti e il privilegio minimo per i team che devono operare in questi account. Suddividendo il flusso di rete in cloud privati virtuali in entrata e in uscita separati (VPCs), è possibile proteggere l'infrastruttura e il traffico sensibili da accessi indesiderati. La rete in entrata è generalmente considerata a maggior rischio e merita routing, monitoraggio e mitigazione appropriati dei potenziali problemi. Questi account dell'infrastruttura erediteranno i guardrail di autorizzazione dall'account di gestione dell'organizzazione e dall'unità organizzativa dell'infrastruttura. I team di rete (e sicurezza) gestiscono la maggior parte dell'infrastruttura di questo account.

Architettura di rete

Sebbene la progettazione e le specifiche della rete non rientrino nell'ambito di questo documento, consigliamo queste tre opzioni per la connettività di rete tra i vari account: peering AWS PrivateLink VPC e. AWS Transit Gateway Le considerazioni importanti da fare nella scelta tra queste opzioni sono le norme operative, i budget e le esigenze specifiche di larghezza di banda.

- Peering VPC – Il modo più semplice per connetterne due VPCs è utilizzare il peering VPC. Una connessione consente la connettività bidirezionale completa tra. VPCs VPCs che si trovano in account separati e Regioni AWS possono anche essere collegati tra loro. Su larga scala, quando ne hai da decine a centinaia VPCs, l'interconnessione con il peering produce una rete di centinaia o migliaia di connessioni peering, il che può essere difficile da gestire e scalare. Il peering VPC viene utilizzato al meglio quando le risorse di un VPC devono comunicare con le risorse di un altro VPC, l'ambiente di entrambi VPCs è controllato e protetto e il numero di connessioni da connettere è inferiore VPCs a 10 (per consentire la gestione individuale di ogni connessione).
- AWS PrivateLink– PrivateLink fornisce connettività privata tra VPCs servizi e applicazioni. Puoi creare la tua applicazione nel tuo VPC e configurarla come un servizio PrivateLink basato su tecnologia (denominato servizio endpoint). Altri AWS principali possono creare una connessione dal proprio VPC al servizio endpoint utilizzando un endpoint VPC di interfaccia o un endpoint Gateway Load Balancer, a seconda del tipo di servizio. Quando si utilizza PrivateLink, il traffico del servizio non attraversa una rete instradabile pubblicamente. Utilizzalo PrivateLink quando disponi di una configurazione client-server in cui desideri fornire a uno o più consumatori l'accesso VPCs unidirezionale a un servizio o a un set di istanze specifico nel VPC del provider di servizi. Questa è anche una buona opzione quando client e server dei due VPCs hanno indirizzi IP sovrapposti, perché PrivateLink utilizza interfacce di rete elastiche all'interno del VPC del client in modo che non vi siano conflitti IP con il provider di servizi.
- AWS Transit Gateway– Transit Gateway offre un hub-and-spoke design per la connessione VPCs e le reti locali come servizio completamente gestito senza la necessità di effettuare il

provisioning di appliance virtuali. AWS gestisce l'elevata disponibilità e scalabilità. Un gateway di transito è una risorsa regionale e può collegarne migliaia VPCs all'interno della stessa Regione AWS. È possibile collegare la connettività ibrida (VPN e AWS Direct Connect connessioni) a un singolo gateway di transito, consolidando e controllando così l'intera configurazione di routing AWS dell'organizzazione in un unico posto. Un gateway di transito risolve la complessità legata alla creazione e alla gestione di più connessioni peering VPC su larga scala. È l'impostazione predefinita per la maggior parte delle architetture di rete, ma esigenze specifiche in termini di costi, larghezza di banda e latenza potrebbero rendere il peering VPC più adatto alle tue esigenze.

VPC in ingresso (ingress)

Il VPC in entrata è destinato ad accettare, ispezionare e instradare le connessioni di rete avviate dall'esterno dell'applicazione. A seconda delle specifiche dell'applicazione, puoi aspettarti di vedere una traduzione degli indirizzi di rete, ovvero una Network Address Translation (NAT) in questo VPC. I log di flusso di questo VPC vengono acquisiti e archiviati nell'account Log Archive.

VPC in uscita (egress)

Il VPC in uscita è destinato a gestire le connessioni di rete avviate dall'interno dell'applicazione. A seconda delle specifiche dell'applicazione, puoi aspettarti di vedere traffico NAT, endpoint VPC Servizio AWS specifici e hosting di endpoint API esterni in questo VPC. I log di flusso di questo VPC vengono acquisiti e archiviati nell'account Log Archive.

VPC di ispezione

Un VPC di ispezione dedicato offre un approccio semplificato e centrale per la gestione delle ispezioni tra VPCs (nella stessa o in diverse Regioni AWS), Internet e reti locali. Per l' AWS SRA, assicuratevi che tutto il traffico intercorrente VPCs passi attraverso il VPC di ispezione ed evitate di utilizzare il VPC di ispezione per qualsiasi altro carico di lavoro.

AWS Network Firewall

AWS Network Firewallè un servizio firewall di rete gestito e ad alta disponibilità per il tuo VPC. Ti consente di implementare e gestire senza problemi l'ispezione dello stato, la prevenzione e il rilevamento delle intrusioni e il filtraggio web per proteggere le tue reti virtuali su. AWSÈ possibile utilizzare Network Firewall per decrittografare le sessioni TLS e ispezionare il traffico in entrata e in uscita. Per ulteriori informazioni sulla configurazione del Network Firewall, consulta il post sul AWS Network Firewall blog — New Managed Firewall Service in VPC.

Utilizzi un firewall in base alla zona di disponibilità nel tuo VPC. Per ogni zona di disponibilità, scegli una sottorete per ospitare l'endpoint firewall che filtra il traffico. L'endpoint firewall in una zona di disponibilità può proteggere tutte le sottoreti all'interno della zona ad eccezione della sottorete in cui si trova. A seconda del caso d'uso e del modello di implementazione, la sottorete del firewall può essere pubblica o privata. Il firewall è completamente trasparente per il flusso di traffico e non esegue la traduzione degli indirizzi di rete, ovvero il Network Address Translation (NAT). Conserva l'indirizzo di origine e di destinazione. In questa architettura di riferimento, gli endpoint del firewall sono ospitati in un VPC di ispezione. Tutto il traffico dal VPC in entrata e verso il VPC in uscita viene instradato attraverso questa sottorete del firewall per l'ispezione.

Network Firewall rende visibile l'attività del firewall in tempo reale attraverso i CloudWatch parametri di Amazon e offre una maggiore visibilità del traffico di rete inviando i log ad Amazon Simple Storage Service (Amazon S3) e Amazon Data CloudWatch Firehose. Network Firewall è interoperabile con l'approccio alla sicurezza esistente, comprese le tecnologie dei partner.AWS Puoi anche importare set di regole Suricata esistenti, che potrebbero essere stati scritti internamente o forniti esternamente da fornitori di terze parti o piattaforme open source.

Nell' AWS SRA, Network Firewall viene utilizzato all'interno dell'account di rete perché la funzionalità del servizio incentrata sul controllo della rete è in linea con l'intento dell'account.

Considerazioni di natura progettuale

- AWS Firewall Manager supporta Network Firewall, quindi puoi configurare e distribuire centralmente le regole del Network Firewall in tutta l'organizzazione. (Per i dettagli, consulta Utilizzo AWS Network Firewall delle politiche in Firewall Manager nella AWS documentazione.) Quando si configura Firewall Manager, viene creato automaticamente un firewall con set di regole negli account e VPCs specificate dall'utente. Inoltre, distribuisce un endpoint in una sottorete dedicata per ogni zona di disponibilità che contiene sottoreti pubbliche. Allo stesso tempo, qualsiasi modifica al set di regole configurato centralmente viene automaticamente aggiornata a valle sui firewall di Firewall di rete implementati.
- Con Firewall di rete sono disponibili diversi modelli di implementazione. Il modello più adatto varia a seconda dei requisiti e del caso d'uso. Considerare i seguenti esempi:
  - Un modello di distribuzione distribuito in cui Network Firewall viene distribuito in singoli VPCs utenti.

  - Un modello di implementazione centralizzato in cui Firewall di rete viene implementato in un VPC centralizzato per il traffico est-ovest (da VPC a VPC) o nord-sud (uscita e ingresso Internet, on-premise).
  - Un modello di implementazione combinato in cui Firewall di rete viene implementato in un VPC centralizzato per il traffico est-ovest e un sottoinsieme del traffico nord-sud.
- Come best practice, non utilizzare la sottorete di Firewall di rete per implementare qualsiasi altro servizio. Questo perché Firewall di rete non è in grado di ispezionare il traffico proveniente da origini o destinazioni all'interno della sottorete del firewall.

Strumento di analisi degli accessi alla rete

Strumento di analisi degli accessi alla rete è una funzionalità di Amazon VPC che identifica gli accessi di rete non intenzionali alle tue risorse. Strumento di analisi degli accessi alla rete può essere utilizzato per convalidare la segmentazione della rete, identificare risorse accessibili da Internet o accessibili solo da intervalli di indirizzi IP attendibili e verificare di disporre di controlli di rete appropriati su tutti i percorsi di rete.

Network Access Analyzer utilizza algoritmi di ragionamento automatizzato per analizzare i percorsi di rete che un pacchetto può percorrere tra le risorse di una AWS rete e produce risultati per i percorsi che corrispondono all'ambito di accesso alla rete definito. Strumento di analisi degli accessi alla rete esegue un'analisi statica di una configurazione di rete, il che significa che nessun pacchetto viene trasmesso nella rete come parte di questa analisi.

Le regole di raggiungibilità della rete Amazon Inspector forniscono una funzionalità correlata. I risultati generati da queste regole vengono utilizzati nell'account dell'applicazione. Sia Network Access Analyzer che Network Reachability utilizzano la tecnologia più recente della AWS comprovable security initiative e applicano questa tecnologia con diverse aree di interesse. Il pacchetto Network Reachability si concentra specificamente sulle EC2 istanze e sulla loro accessibilità a Internet.

L'account di rete definisce l'infrastruttura di rete critica che controlla il traffico in entrata e in uscita dall'ambiente. AWS Questo traffico deve essere monitorato attentamente. Nell' AWS SRA, Network Access Analyzer viene utilizzato all'interno dell'account di rete per aiutare a identificare accessi involontari alla rete, identificare le risorse accessibili a Internet tramite gateway Internet e verificare che i controlli di rete appropriati, come i firewall di rete e i gateway NAT, siano presenti su tutti i percorsi di rete tra risorse e gateway Internet.

> **Considerazione di natura progettuale**
>
> Network Access Analyzer è una funzionalità di Amazon VPC e può essere utilizzata in Account AWS qualsiasi ambiente che disponga di un VPC. Gli amministratori di rete possono avvalersi di ruoli IAM ben definiti e trasversali tra account per verificare che i percorsi di rete approvati vengano applicati all'interno di ciascuno di essi. Account AWS

AWS RAM

AWS Resource Access Manager(AWS RAM) ti aiuta a condividere in modo sicuro le AWS risorse che crei l'una con l'altra. Account AWS Account AWSAWS RAM fornisce una posizione centrale per gestire la condivisione delle risorse e standardizzare questa esperienza tra gli account. Ciò semplifica la gestione delle risorse sfruttando al contempo l'isolamento amministrativo e di fatturazione e riduce la portata dei vantaggi di contenimento dell'impatto offerti da una strategia multi-account. Se il tuo account è gestito da AWS Organizations, ti AWS RAM consente di condividere le risorse con tutti gli account dell'organizzazione o solo con gli account all'interno di una o più unità organizzative specificate (OUs). Puoi anche condividere con ID specifici Account AWS per account, indipendentemente dal fatto che l'account faccia parte di un'organizzazione. Puoi anche condividere alcuni tipi di risorse supportati con ruoli e utenti IAM specifici.

AWS RAM consente di condividere risorse che non supportano le policy basate sulle risorse IAM, come le sottoreti VPC e le regole Route 53. Inoltre, con AWS RAM, i proprietari di una risorsa possono vedere quali responsabili hanno accesso alle singole risorse che hanno condiviso. I responsabili IAM possono recuperare direttamente l'elenco delle risorse condivise con loro, cosa che non possono fare con le risorse condivise dalle policy delle risorse IAM. Se AWS RAM viene utilizzato per condividere risorse all'esterno AWS dell'organizzazione, viene avviato un processo di invito. Il destinatario deve accettare l'invito prima di concedere l'accesso alle risorse. Ciò fornisce controlli ed equilibri aggiuntivi.

AWS RAM viene richiamato e gestito dal proprietario della risorsa, nell'account in cui viene distribuita la risorsa condivisa. Un caso d'uso comune AWS RAM illustrato nell' AWS SRA è che gli amministratori di rete condividano sottoreti VPC e gateway di transito con l'intera organizzazione. AWS Ciò offre la possibilità di disaccoppiare le funzioni di gestione della rete Account AWS e aiuta a raggiungere la separazione delle mansioni. Per ulteriori informazioni sulla condivisione VPC, consulta il AWS post del blog Condivisione VPC: un nuovo approccio alla gestione di più account e VPC e al white paper sull'infrastruttura di rete.AWS

Considerazione di natura progettuale

Sebbene AWS RAM il servizio sia distribuito solo all'interno dell'account di rete nell' AWS SRA, in genere viene distribuito in più di un account. Ad esempio, è possibile centralizzare la gestione del data lake su un singolo account di data lake e quindi condividere le risorse del catalogo AWS Lake Formation dati (database e tabelle) con altri account dell'organizzazione. AWS Per ulteriori informazioni, consulta la AWS Lake Formation documentazione e il post AWS sul blog Condividi in modo sicuro i tuoi dati durante Account AWS l'utilizzo. AWS Lake Formation Inoltre, gli amministratori della sicurezza possono AWS RAM seguire le migliori pratiche quando creano una AWS Autorità di certificazione privata gerarchia. CAs può essere condiviso con terze parti esterne, che possono emettere certificati senza avere accesso alla gerarchia delle CA. Ciò consente alle organizzazioni di origine di limitare e revocare l'accesso di terze parti.

Accesso verificato da AWS

Accesso verificato da AWSfornisce un accesso sicuro alle applicazioni e alle risorse aziendali senza una VPN. Migliora il livello di sicurezza e aiuta ad applicare l'accesso Zero Trust valutando ogni richiesta di accesso in tempo reale rispetto ai requisiti predefiniti. È possibile definire una policy di accesso unica per ogni applicazione con condizioni basate sui dati di identità e sulla postura del dispositivo. Verified Access fornisce un accesso sicuro alle applicazioni HTTP (S), come le applicazioni basate su browser, e alle applicazioni non HTTP (S) tramite protocolli TCP, SSH e RDP per applicazioni come repository Git, database e gruppi di istanze. EC2 È possibile accedervi utilizzando un terminale a riga di comando o da un'applicazione desktop. Accesso verificato semplifica inoltre le operazioni di sicurezza aiutando gli amministratori a impostare e monitorare in modo efficiente le policy di accesso. Ciò consente di risparmiare tempo per aggiornare le policy, rispondere agli incidenti di sicurezza e connettività e verificare gli standard di conformità. Verified Access supporta anche l'integrazione con AWS WAF per aiutarti a filtrare le minacce più comuni come SQL injection e cross-site scripting (XSS). Verified Access è perfettamente integrato con AWS IAM Identity Center, il che consente agli utenti di autenticarsi con provider di identità di terze parti basati su SAML (). IdPs Se disponi già di una soluzione IdP personalizzata compatibile con OpenID Connect (OIDC), Accesso verificato può anche autenticare gli utenti connettendosi direttamente con il tuo IdP. Accesso verificato registra ogni tentativo di accesso in modo da poter rispondere rapidamente agli incidenti di sicurezza e alle richieste di controllo. Verified Access supporta la

consegna di questi log ad Amazon Simple Storage Service (Amazon S3), Amazon CloudWatch Logs e Amazon Data Firehose.

Accesso verificato supporta due modelli applicativi aziendali comuni: interni e rivolti a Internet. Accesso verificato si integra con le applicazioni tramite Application Load Balancer o interfacce di rete elastiche. Se utilizzi un Application Load Balancer, Verified Access richiede un load balancer interno. Poiché Verified Access supporta AWS WAF a livello di istanza, un'applicazione esistente con AWS WAF integrazione con un Application Load Balancer può spostare le policy dal load balancer all'istanza Verified Access. Un'applicazione aziendale è rappresentata come un endpoint di Accesso verificato. Ogni endpoint è associato a un gruppo di Accesso verificato ed eredita la policy di accesso per il gruppo. Un gruppo di Accesso verificato è una raccolta di endpoint di Accesso verificato e una policy di Accesso verificato a livello di gruppo. I gruppi semplificano la gestione delle policy e consentono agli amministratori IT di impostare criteri di base. I proprietari delle applicazioni possono definire ulteriormente policy granulari in base alla sensibilità dell'applicazione.

Nell' AWS SRA, l'accesso verificato è ospitato all'interno dell'account di rete. Il team IT centrale imposta configurazioni gestite centralmente. Ad esempio, potrebbero collegare provider affidabili come provider di identità (ad esempio Okta) e provider di attendibilità dei dispositivi (ad esempio, Jamf), creare gruppi e determinare la policy a livello di gruppo. Queste configurazioni possono quindi essere condivise con decine, centinaia o migliaia di account di carico di lavoro utilizzando. AWS RAM Ciò consente ai team applicativi di gestire gli endpoint sottostanti che gestiscono le loro applicazioni senza sovraccaricare gli altri team. AWS RAM offre un modo scalabile per sfruttare Verified Access per le applicazioni aziendali ospitate in diversi account di carico di lavoro.

> **Considerazione di natura progettuale**
>
> Puoi raggruppare gli endpoint per applicazioni che hanno requisiti di sicurezza simili per semplificare l'amministrazione delle policy e quindi condividere il gruppo con gli account delle applicazioni. Tutte le applicazioni del gruppo condividono la policy di gruppo. Se un'applicazione del gruppo richiede una policy specifica a causa di un caso limite, è possibile applicare una policy a livello di applicazione per quell'applicazione.

Amazon VPC Lattice

Amazon VPC Lattice è un servizio di rete di applicazioni che connette, monitora e protegge le comunicazioni. service-to-service Un servizio, spesso chiamato microservizio, è un'unità

software distribuibile in modo indipendente che svolge un'attività specifica. VPC Lattice gestisce automaticamente la connettività di rete e il routing a livello di applicazione tra i servizi VPCs e Account AWS senza la necessità di gestire la connettività di rete sottostante, i bilanciatori del carico frontend o i proxy sidecar. Fornisce un proxy a livello di applicazione completamente gestito che fornisce il routing a livello di applicazione in base alle caratteristiche della richiesta, come percorsi e intestazioni. VPC Lattice è integrato nell'infrastruttura VPC, quindi fornisce un approccio coerente su un'ampia gamma di tipi di elaborazione come Amazon Elastic Compute Cloud (Amazon), Amazon EC2 Elastic Kubernetes Service (Amazon EKS) e. AWS Lambda VPC Lattice supporta anche il routing ponderato e le implementazioni in stile Canary. blue/green È possibile utilizzare VPC Lattice per creare una rete di servizi con un limite logico che implementa automaticamente il rilevamento e la connettività dei servizi. VPC Lattice si integra con IAM per l' service-to-serviceautenticazione e l'autorizzazione utilizzando le politiche di autenticazione.

VPC Lattice si integra con AWS RAM per consentire la condivisione di servizi e reti di servizi. AWS SRA rappresenta un'architettura distribuita in cui sviluppatori o proprietari di servizi creano servizi VPC Lattice nel proprio account Application. I proprietari dei servizi definiscono gli ascoltatori, le regole di routing e i gruppi di destinazione insieme alle policy di autenticazione. Quindi condividono i servizi con altri account e li associano alle reti di servizi VPC Lattice. Queste reti vengono create dagli amministratori di rete nell'account di rete e condivise con l'account dell'applicazione. Gli amministratori di rete configurano le policy di autenticazione e il monitoraggio a livello di rete del servizio. Gli amministratori associano VPCs i servizi VPC Lattice a una o più reti di servizi. Per una panoramica dettagliata di questa architettura distribuita, consulta il post del AWS blog Crea una connettività multi-VPC multi-account sicura per le tue applicazioni con Amazon VPC Lattice

Considerazioni di natura progettuale

- A seconda del modello operativo di servizio o della visibilità della rete di servizi dell'organizzazione, gli amministratori di rete possono condividere le proprie reti di servizi e dare ai proprietari dei servizi il controllo necessario per associare i propri servizi e a queste reti di servizi. VPCs In alternativa, i proprietari dei servizi possono condividere i propri servizi e gli amministratori di rete possono associare i servizi alle reti di servizi.
- Un client può inviare richieste ai servizi associati a una rete di servizi solo se il client si trova in un VPC associato alla stessa rete di servizi. Il traffico client che attraversa una connessione peering VPC o un gateway di transito viene negato.

Sicurezza edge

La sicurezza edge prevede generalmente tre tipi di protezione: distribuzione sicura dei contenuti, protezione a livello di rete e di applicazione e mitigazione della denial of service (S) distribuita. DDo Contenuti come dati, video, applicazioni APIs devono essere distribuiti in modo rapido e sicuro, utilizzando la versione consigliata di TLS per crittografare le comunicazioni tra gli endpoint. Il contenuto dovrebbe inoltre avere restrizioni di accesso tramite cookie firmati e URLs firmati e autenticazione tramite token. La sicurezza a livello di applicazione dovrebbe essere progettata per controllare il traffico dei bot, bloccare schemi di attacco comuni come iniezione SQL o scripting cross-site (XSS) e fornire visibilità del traffico Web. A livello perimetrale, la mitigazione DDo S fornisce un importante livello di difesa che garantisce la disponibilità continua delle operazioni e dei servizi aziendali cruciali. Le applicazioni APIs devono essere protette dai flood SYN, dai flood UDP o da altri attacchi di riflessione e devono essere dotate di una mitigazione in linea per bloccare gli attacchi di base a livello di rete.

AWS offre diversi servizi per contribuire a fornire un ambiente sicuro, dal cloud principale alla periferia della rete. AWS Amazon CloudFront, AWS Certificate Manager (ACM) e Amazon Route 53 collaborano per contribuire a creare un perimetro di sicurezza flessibile e stratificato. AWS Shield AWS WAF Con CloudFront APIs, i contenuti o le applicazioni possono essere distribuiti tramite HTTPS utilizzando TLSv1 .3 per crittografare e proteggere la comunicazione tra client di visualizzazione e. CloudFront Puoi utilizzare ACM per creare un certificato SSL personalizzato e distribuirlo gratuitamente su una distribuzione. CloudFront ACM gestisce automaticamente il rinnovo dei certificati. Shield è un servizio di protezione DDo S gestito che aiuta a proteggere le applicazioni in esecuzione su AWS. Fornisce un rilevamento dinamico e mitigazioni automatiche in linea che riducono al minimo i tempi di inattività e la latenza delle applicazioni. AWS WAF consente di creare regole per filtrare il traffico Web in base a condizioni specifiche (indirizzi IP, intestazioni e corpo HTTP o personalizzati URIs), attacchi Web comuni e bot pervasivi. Route 53 è un servizio Web DNS altamente scalabile e disponibile. Route 53 collega le richieste degli utenti alle applicazioni Internet eseguite in locale o in AWS locale. L' AWS SRA adotta un'architettura di ingresso di rete centralizzata utilizzando AWS Transit Gateway, ospitata all'interno dell'account di rete, in modo che anche l'infrastruttura di sicurezza perimetrale sia centralizzata in questo account.

Amazon CloudFront

Amazon CloudFront è una rete di distribuzione dei contenuti (CDN) sicura che fornisce una protezione intrinseca contro il livello di rete comune e i tentativi di trasporto DDo S. Puoi distribuire i tuoi contenuti o le tue applicazioni utilizzando i certificati TLS e le funzionalità TLS avanzate vengono

abilitate automaticamente. APIs È possibile utilizzare AWS Certificate Manager (ACM) per creare un certificato TLS personalizzato e applicare le comunicazioni HTTPS tra i visualizzatori e CloudFront, come descritto più avanti nella sezione ACM. È inoltre possibile richiedere che le comunicazioni tra CloudFront e l'origine personalizzata implementino la crittografia in transito. end-to-end In questo scenario, è necessario installare un certificato TLS sul server di origine. Se l'origine è un sistema di bilanciamento del carico elastico, è possibile utilizzare un certificato generato da ACM o un certificato convalidato da un'autorità di certificazione (CA) di terze parti e importato in ACM. Se gli endpoint dei siti Web con bucket S3 fungono da origine per CloudFront, non puoi configurare CloudFront l'utilizzo di HTTPS con la tua origine, poiché Amazon S3 non supporta HTTPS per gli endpoint dei siti Web. (Tuttavia, puoi comunque richiedere HTTPS tra i visualizzatori e.) CloudFront Per tutte le origini che supportano l'installazione di certificati HTTPS, è necessario utilizzare un certificato firmato da un'autorità di certificazione (CA) di terze parti attendibile.

CloudFront offre diverse opzioni per proteggere e limitare l'accesso ai tuoi contenuti. Ad esempio, può limitare l'accesso alla tua origine Amazon S3 utilizzando cookie firmati URLs e firmati. Per ulteriori informazioni, consulta Configurare l'accesso sicuro e limitare l'accesso ai contenuti nella CloudFront documentazione.

L' AWS SRA illustra le CloudFront distribuzioni centralizzate nell'account di rete perché si allineano al modello di rete centralizzato implementato utilizzando. AWS Transit Gateway Implementando e gestendo CloudFront le distribuzioni nell'account di rete, si ottengono i vantaggi dei controlli centralizzati. Puoi gestire tutte le CloudFront distribuzioni in un unico posto, il che semplifica il controllo degli accessi, la configurazione delle impostazioni e il monitoraggio dell'utilizzo su tutti gli account. Inoltre, puoi gestire i certificati ACM, i record DNS e la CloudFront registrazione da un unico account centralizzato.

La dashboard CloudFront di sicurezza offre AWS WAF visibilità e controlli direttamente nella distribuzione. CloudFront Ottieni visibilità sulle principali tendenze di sicurezza della tua applicazione, sul traffico consentito e bloccato e sull'attività dei bot. Puoi utilizzare strumenti investigativi come analizzatori visivi dei log e controlli di blocco integrati per isolare i modelli di traffico e bloccare il traffico senza interrogare i log o scrivere regole di sicurezza.

Considerazioni di natura progettuale

- In alternativa, è possibile eseguire la distribuzione CloudFront come parte dell'applicazione nell'account dell'applicazione. In questo scenario, il team dell'applicazione prende decisioni come la modalità di CloudFront distribuzione delle distribuzioni, determina le politiche di cache appropriate e si assume la responsabilità della governance, del controllo e del

monitoraggio delle distribuzioni. CloudFront Distribuendo CloudFront le distribuzioni su più account, è possibile beneficiare di quote di servizio aggiuntive. Come altro vantaggio, puoi utilizzare la configurazione intrinseca e automatizzata CloudFront di Origin Access Identity (OAI) e Origin Access Control (OAC) per limitare l'accesso alle origini di Amazon S3.

- Quando distribuisci contenuti web tramite un CDN, ad esempio CloudFront, devi impedire agli spettatori di aggirare il CDN e accedere direttamente ai tuoi contenuti di origine. Per ottenere questa restrizione di accesso all'origine, potete utilizzare CloudFront e aggiungere intestazioni personalizzate e AWS WAF verificare le intestazioni prima di inoltrare le richieste all'origine personalizzata. Per una spiegazione dettagliata di questa soluzione, consulta il post del blog AWS sulla sicurezza How to enhance Amazon CloudFront Origin Security with AWS WAF and Gestione dei segreti AWS. Un metodo alternativo consiste nel limitare solo l'elenco dei CloudFront prefissi nel gruppo di sicurezza associato all'Application Load Balancer. Ciò contribuirà a garantire che solo una CloudFront distribuzione possa accedere al load balancer.

AWS WAF

AWS WAFè un firewall per applicazioni Web che aiuta a proteggere le applicazioni Web da exploit Web, come vulnerabilità comuni e bot, che potrebbero influire sulla disponibilità delle applicazioni, compromettere la sicurezza o consumare risorse eccessive. Può essere integrato con una CloudFront distribuzione Amazon, un'API REST di Amazon API Gateway, un Application Load Balancer, un'API GraphQL AWS AppSync , un pool di utenti Amazon Cognito e il servizio. AWS App Runner

AWS WAF utilizza le liste di controllo degli accessi Web (ACLs) per proteggere un insieme di risorse. AWS Un ACL Web è un insieme di regole che definisce i criteri di ispezione e un'azione associata da intraprendere (bloccare, consentire, contare o eseguire il controllo dei bot) se una richiesta Web soddisfa i criteri. AWS WAF fornisce una serie di regole gestite che forniscono protezione dalle vulnerabilità comuni delle applicazioni. Queste regole sono curate e gestite da AWS e AWS Partner. AWS WAF offre anche un potente linguaggio di regole per la creazione di regole personalizzate. Puoi utilizzare regole personalizzate per scrivere criteri di ispezione adatti alle tue esigenze particolari. Gli esempi includono restrizioni IP, restrizioni geografiche e versioni personalizzate delle regole gestite che meglio si adattano al comportamento specifico dell'applicazione.

AWS WAF fornisce una serie di regole intelligenti gestite a più livelli per bot comuni e mirati e la protezione dall'acquisizione di account (ATP). Quando utilizzi i gruppi di regole ATP e il rilevamento

dei bot ti viene addebitata una quota di abbonamento e una commissione per l'ispezione del traffico. Pertanto, consigliamo di monitorare il traffico e decidere poi cosa utilizzare. Puoi utilizzare le dashboard di gestione dei bot e acquisizione degli account disponibili gratuitamente sulla AWS WAF console per monitorare queste attività e quindi decidere se è necessario un gruppo di regole intelligente di livello. AWS WAF

Nell' AWS SRA, AWS WAF è integrato con l'account di CloudFront rete. In questa configurazione, l'elaborazione delle AWS WAF regole avviene nelle edge location anziché all'interno del VPC. Ciò consente di filtrare il traffico dannoso più vicino all'utente finale che ha richiesto il contenuto e aiuta a limitare l'ingresso del traffico dannoso nella rete principale.

Puoi inviare AWS WAF log completi a un bucket S3 nell'account Log Archive configurando l'accesso tra account al bucket S3. Per ulteriori informazioni, consulta l'articolo di re:POST su questo argomento.AWS

Considerazioni di natura progettuale

- In alternativa alla distribuzione AWS WAF centralizzata nell'account di rete, alcuni casi d'uso sono meglio soddisfatti mediante la distribuzione AWS WAF nell'account dell'applicazione. Ad esempio, puoi scegliere questa opzione quando distribuisci le tue CloudFront distribuzioni nel tuo account Application o disponi di Application Load Balancer rivolti al pubblico o se utilizzi API Gateway davanti alle tue applicazioni web. Se decidete di effettuare la distribuzione AWS WAF in ogni account dell'Applicazione, utilizzate AWS Firewall Manager per gestire AWS WAF le regole di questi account dall'account Security Tooling centralizzato.
- È inoltre possibile aggiungere AWS WAF regole generali a CloudFront livello e AWS WAF regole aggiuntive specifiche dell'applicazione in una risorsa regionale come Application Load Balancer o il gateway API.

AWS Shield

AWS Shieldè un servizio di protezione DDo S gestito che protegge le applicazioni in esecuzione su. AWS Esistono due livelli di Shield: Shield Standard e Shield Advanced. Shield Standard offre a tutti AWS i clienti protezione dagli eventi dell'infrastruttura più comuni (livelli 3 e 4) senza costi aggiuntivi. Shield Advanced offre mitigazioni automatiche più sofisticate per gli eventi non autorizzati che prendono di mira le applicazioni su zone ospitate protette di Amazon EC2, Elastic Load Balancing

(Elastic Load Balancing) e CloudFront Route AWS Global Accelerator 53. Se possiedi siti Web ad alta visibilità o sei soggetto a frequenti attacchi DDo S, puoi prendere in considerazione le funzionalità aggiuntive fornite da Shield Advanced.

Puoi utilizzare la funzionalità di mitigazione automatica Shield Advanced application layer DDo S per configurare Shield Advanced in modo che risponda automaticamente agli attacchi del livello applicativo (livello 7) contro le tue CloudFront distribuzioni protette, i sistemi di bilanciamento del carico Elastic Load Balancing (Elastic Load Balancing) (Application, Network e Classic), le zone ospitate di Amazon Route 53, gli indirizzi IP Amazon Elastic e gli acceleratori standard. EC2 AWS Global Accelerator Quando abiliti questa funzionalità, Shield Advanced genera automaticamente AWS WAF regole personalizzate per mitigare gli attacchi DDo S. Shield Advanced ti dà anche accesso al AWS Shield Response Team (SRT). Puoi contattare SRT in qualsiasi momento per creare e gestire mitigazioni personalizzate per la tua applicazione o durante un attacco S attivo DDo. Se desideri che SRT monitori in modo proattivo le tue risorse protette e ti contatti durante un tentativo DDo S, valuta la possibilità di abilitare la funzione di coinvolgimento proattivo.

Considerazioni di natura progettuale

- Se hai carichi di lavoro gestiti da risorse connesse a Internet nell'account dell'applicazione, come un Application Load Balancer o un Network Load CloudFront Balancer, configura Shield Advanced nell'account Application e aggiungi tali risorse alla protezione Shield. Puoi AWS Firewall Manager utilizzarle per configurare queste opzioni su larga scala.
- Se nel flusso di dati sono presenti più risorse, ad esempio una CloudFront distribuzione davanti a un Application Load Balancer, utilizza solo la risorsa entry-point come risorsa protetta. In questo modo non dovrai pagare due volte le tariffe di Shield Data Transfer Out (DTO) per due risorse.
- Shield Advanced registra i parametri che puoi monitorare in Amazon CloudWatch. (Per ulteriori informazioni, consulta Monitoring with Amazon CloudWatch nella AWS documentazione.) Imposta CloudWatch allarmi per ricevere notifiche SNS al tuo centro di sicurezza quando viene rilevato un evento DDo S. In caso di sospetto evento DDo S, contatta il team di AWS Enterprise Support compilando un ticket di supporto e assegnandogli la massima priorità. Il team di Supporto Enterprise includerà lo Shield Response Team (SRT) nella gestione dell'evento. Inoltre, puoi preconfigurare la funzione AWS Shield Engagement Lambda per creare un ticket di supporto e inviare un'e-mail al team SRT.

AWS Certificate Manager (ACM)

AWS Certificate Manager(ACM) consente di fornire, gestire e distribuire certificati TLS pubblici e privati da utilizzare con le risorse interne Servizi AWS connesse. Con ACM, puoi richiedere rapidamente un certificato, distribuirlo su AWS risorse integrate con ACM, come sistemi di bilanciamento del carico Elastic Load Balancing, distribuzioni CloudFront e su Amazon APIs API Gateway, e lasciare che ACM gestisca i rinnovi dei certificati. Quando richiedi certificati pubblici ACM, non è necessario generare una key pair o una richiesta di firma del certificato (CSR), inviare una CSR a un'autorità di certificazione (CA) o caricare e installare il certificato quando viene ricevuto. ACM offre anche la possibilità di importare certificati TLS emessi da terze parti CAs e di distribuirli con i servizi integrati ACM. Quando utilizzi ACM per gestire i certificati, le chiavi private dei certificati vengono protette e archiviate in modo sicuro utilizzando una crittografia avanzata e le best practice di gestione delle chiavi. Con ACM non sono previsti costi aggiuntivi per la fornitura di certificati pubblici e ACM gestisce il processo di rinnovo.

ACM viene utilizzato nell'account di rete per generare un certificato TLS pubblico, che a sua volta viene utilizzato dalle CloudFront distribuzioni per stabilire la connessione HTTPS tra i visualizzatori e. CloudFront Per ulteriori informazioni, consulta la documentazione relativa ad CloudFront .

> **Considerazione di natura progettuale**
>
> Per i certificati diretti all'esterno, ACM deve trovarsi nello stesso account delle risorse per le quali fornisce i certificati. I certificati non possono essere condivisi tra account.

Amazon Route 53

Amazon Route 53 è un servizio Web DNS altamente scalabile e disponibile. Puoi utilizzare Route 53 per eseguire tre funzioni principali in qualsiasi combinazione: registrazione dominio, routing DNS e controllo dell'integrità.

Puoi utilizzare Route 53 come servizio DNS per mappare i nomi di dominio alle tue EC2 istanze, ai bucket S3, alle distribuzioni e ad altre risorse. CloudFront AWS La natura distribuita dei server AWS DNS aiuta a garantire che gli utenti finali vengano indirizzati alla tua applicazione in modo coerente. Funzionalità come il controllo del flusso di traffico e del routing della Route 53 aiutano a migliorare l'affidabilità. Se l'endpoint dell'applicazione principale diventa non disponibile, puoi configurare il failover per reindirizzare gli utenti verso una posizione alternativa. Route 53 Resolver fornisce DNS ricorsivo per il tuo VPC e le tue reti locali tramite o VPN gestita. AWS Direct Connect AWS

Utilizzando il servizio IAM con Route 53, ottieni un controllo dettagliato su chi può aggiornare i tuoi dati DNS. È possibile abilitare la firma DNSSEC (DNS Security Extensions) per consentire ai risolutori DNS di accertarsi che una risposta DNS provenga da Route 53 e che non sia stata manomessa.

Route 53 Resolver DNS Firewall offre protezione per le richieste DNS in uscita provenienti da... VPCs Queste richieste vengono instradate tramite il risolutore Route 53 per la risoluzione dei nomi di dominio. Un uso principale delle protezioni DNS Firewall è quello di aiutare a prevenire l'esfiltrazione DNS dei dati. Con DNS Firewall, è possibile monitorare e controllare i domini su cui le applicazioni possono eseguire query. Puoi negare l'accesso ai domini che sai essere non validi e consentire il passaggio di tutte le altre query. In alternativa, è possibile rifiutare l'accesso a tutti i domini ad eccezione di quelli che consideri esplicitamente attendibili. È possibile utilizzare DNS Firewall anche per bloccare le richieste di risoluzione alle risorse in zone ospitate private (condivise o locali), inclusi i nomi degli endpoint VPC. Può anche bloccare le richieste di nomi di istanze pubbliche o private. EC2

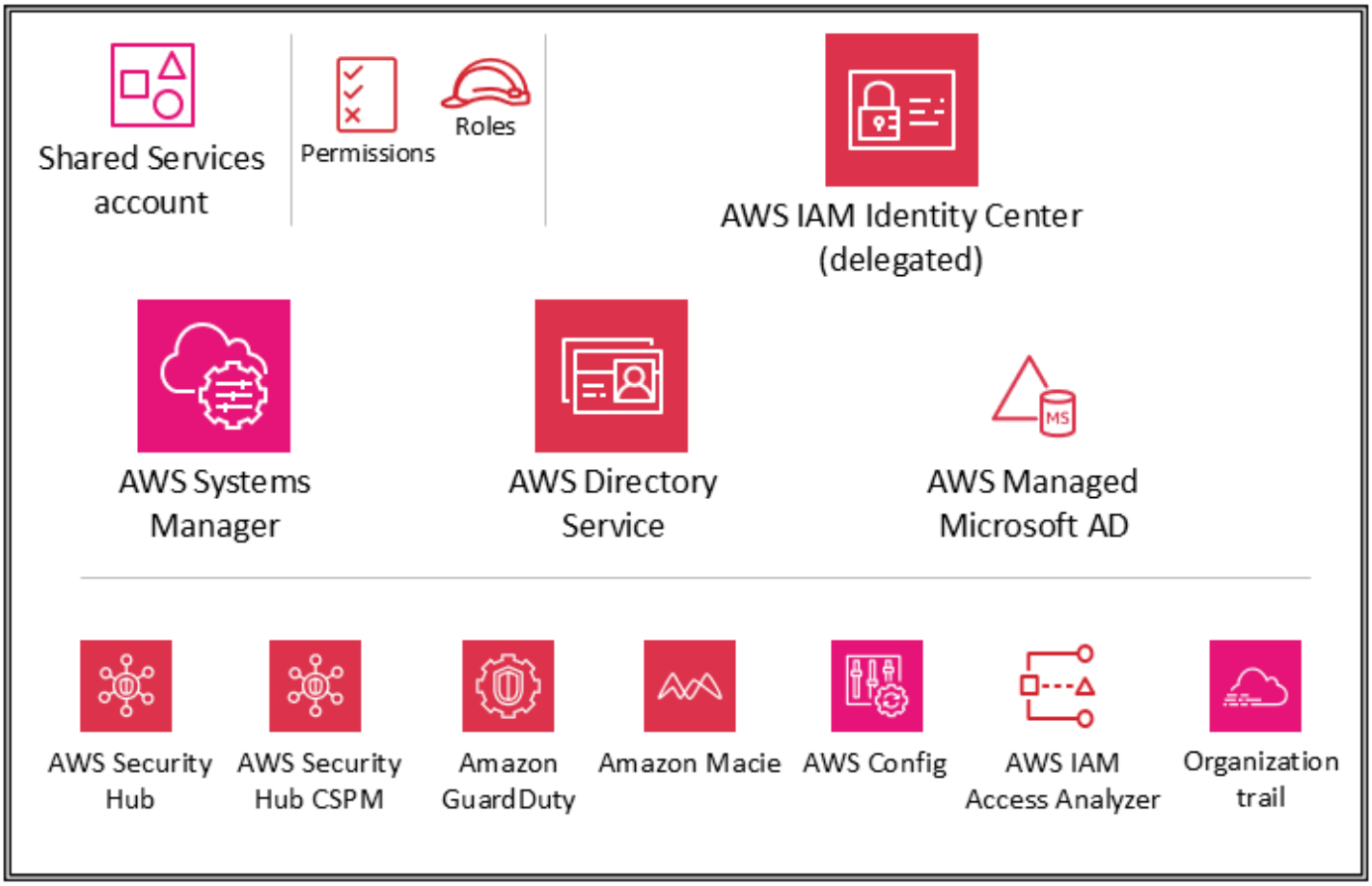
I risolutori Route 53 vengono creati di default come parte di ogni VPC. Nell' AWS SRA, Route 53 viene utilizzata nell'account di rete principalmente per la funzionalità DNS Firewall.

> **Considerazione di natura progettuale**
>
> DNS Firewall ed AWS Network Firewall entrambi offrono il filtraggio dei nomi di dominio, ma per diversi tipi di traffico. È possibile utilizzare DNS Firewall e Network Firewall insieme per configurare il filtraggio basato sul dominio per il traffico a livello di applicazione su due diversi percorsi di rete:
>
> - DNS Firewall fornisce il filtro per le query DNS in uscita che passano attraverso il Route 53 Resolver dalle applicazioni interne al tuo. VPCs È inoltre possibile configurare DNS Firewall per inviare risposte personalizzate per le query a nomi di dominio bloccati.
> - Firewall di rete fornisce filtri sia per il traffico a livello di rete che di applicazione, ma non dispone di visibilità sulle query eseguite dal risolutore Route 53.

Infrastruttura organizzativa — account Shared Services

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

Il diagramma seguente illustra i servizi AWS di sicurezza configurati nell'account Shared Services.



L'account Shared Services fa parte dell'unità organizzativa dell'infrastruttura e il suo scopo è supportare i servizi utilizzati da più applicazioni e team per fornire i propri risultati. Ad esempio, i servizi di directory (Active Directory), i servizi di messaggistica e i servizi di metadati rientrano in questa categoria. L' AWS SRA evidenzia i servizi condivisi che supportano i controlli di sicurezza. Sebbene gli account di rete facciano anche parte dell'unità organizzativa dell'infrastruttura, vengono rimossi dall'account Shared Services per supportare la separazione delle funzioni. I team che gestiranno questi servizi non necessitano di autorizzazioni o accesso agli account di rete.

AWS Systems Manager

AWS Systems Manager(incluso anche nell'account di gestione dell'organizzazione e nell'account dell'applicazione) offre una raccolta di funzionalità che consentono la visibilità e il controllo delle AWS risorse. Una di queste funzionalità, Systems Manager Explorer, è una dashboard operativa personalizzabile che riporta informazioni sulle AWS risorse. È possibile sincronizzare i dati operativi tra tutti gli account AWS dell'organizzazione utilizzando AWS Organizations Systems Manager

Explorer. Systems Manager viene distribuito nell'account Shared Services tramite la funzionalità di amministratore delegato in. AWS Organizations

Systems Manager ti aiuta a mantenere la sicurezza e la conformità scansionando le istanze gestite e segnalando (o adottando azioni correttive) su eventuali violazioni delle policy rilevate. Associando Systems Manager alle implementazioni appropriate nei singoli membri Account AWS (ad esempio, l'account Application), è possibile coordinare la raccolta dei dati di inventario delle istanze e centralizzare l'automazione come l'applicazione di patch e gli aggiornamenti di sicurezza.

AWS Managed Microsoft AD

AWS Directory Service for Microsoft Active Directory, noto anche come AWS Managed Microsoft AD, consente ai carichi di lavoro e alle risorse compatibili con le directory di utilizzare Active Directory gestito su. AWS AWS Puoi utilizzarlo AWS Managed Microsoft AD per aggiungere istanze Amazon EC2 for Windows Server, Amazon EC2 per Linux e Amazon RDS for SQL Server al tuo dominio e AWS utilizzare servizi di elaborazione per utenti finali (EUC), come WorkSpacesAmazon, con utenti e gruppi di Active Directory.

AWS Managed Microsoft AD ti aiuta a estendere il tuo Active Directory esistente AWS e a utilizzare le credenziali utente locali esistenti per accedere alle risorse cloud. Puoi anche amministrare utenti, gruppi, applicazioni e sistemi locali senza la complessità dell'esecuzione e della manutenzione di un Active Directory locale ad alta disponibilità. Puoi aggiungere i computer, i laptop e le stampanti esistenti a un dominio. AWS Managed Microsoft AD

AWS Managed Microsoft AD è basato su Microsoft Active Directory e non richiede la sincronizzazione o la replica dei dati dall'Active Directory esistente al cloud. È possibile utilizzare strumenti e funzionalità di amministrazione familiari di Active Directory, come Group Policy Objects (GPOs), trust di dominio, policy granulari in materia di password, Managed Service Account di gruppo (gMSAs), estensioni dello schema e Single Sign-On basato su Kerberos. È inoltre possibile delegare attività amministrative e autorizzare l'accesso utilizzando i gruppi di sicurezza di Active Directory.

La replica in più regioni consente di distribuire e utilizzare una singola directory su più aree. AWS Managed Microsoft AD Regioni AWS In questo modo è più semplice ed economico distribuire e gestire i carichi di lavoro Microsoft Windows e Linux a livello globale. Quando si utilizza la funzionalità di replica automatizzata in più regioni, si ottiene una maggiore resilienza mentre le applicazioni utilizzano una directory locale per prestazioni ottimali.

AWS Managed Microsoft AD supporta LDAP (Lightweight Directory Access Protocol) su SSL/TLS, noto anche come LDAPS, sia nei ruoli client che server. Quando funge da server, AWS

Managed Microsoft AD supporta LDAPS sulle porte 636 (SSL) e 389 (TLS). È possibile abilitare le comunicazioni LDAPS lato server installando un certificato sui controller di AWS Managed Microsoft AD dominio da un'autorità di certificazione (CA) AWS basata su Active Directory Certificate Services (AD CS). Quando funge da client, AWS Managed Microsoft AD supporta LDAPS sulle porte 636 (SSL). È possibile abilitare le comunicazioni LDAPS lato client registrando i certificati CA degli emittenti dei certificati del server nella directory e quindi abilitando LDAPS nella directory AWS.

Nell' AWS SRA, Directory Service viene utilizzato all'interno dell'account Shared Services per fornire servizi di dominio per carichi di lavoro compatibili con Microsoft su più account membri. AWS

> Considerazione di natura progettuale
>
> Puoi concedere agli utenti di Active Directory locali l'accesso per accedere a Console di gestione AWS and AWS Command Line Interface (AWS CLI) con le loro credenziali Active Directory esistenti utilizzando IAM Identity Center e selezionando come origine dell'identità. AWS Managed Microsoft AD Ciò consente agli utenti di assumere uno dei ruoli loro assegnati al momento dell'accesso e di accedere alle risorse e agire sulle risorse in base alle autorizzazioni definite per il ruolo. Un'opzione alternativa consiste nell'utilizzare per consentire AWS Managed Microsoft AD agli utenti di assumere un ruolo IAM.

Centro identità IAM

L' AWS SRA utilizza la funzionalità di amministratore delegato supportata da AWS IAM Identity Center per delegare la maggior parte dell'amministrazione di IAM Identity Center all'account Shared Services. Ciò consente di limitare il numero di utenti che richiedono l'accesso all'account di gestione dell'organizzazione. IAM Identity Center deve ancora essere abilitato nell'account di gestione dell'organizzazione per eseguire determinate attività, inclusa la gestione dei set di autorizzazioni forniti all'interno dell'account di gestione dell'organizzazione.

Il motivo principale per utilizzare l'account Shared Services come amministratore delegato per IAM Identity Center è la posizione di Active Directory. Se prevedi di utilizzare Active Directory come fonte di identità IAM Identity Center, dovrai individuare la directory nell'account membro che hai designato come account amministratore delegato di IAM Identity Center. Nell' AWS SRA, l'account Shared Services ospita AWS Managed Microsoft AD, quindi tale account diventa amministratore delegato per IAM Identity Center.

IAM Identity Center supporta la registrazione di un singolo account membro come amministratore delegato contemporaneamente. Puoi registrare un account membro solo quando accedi con le credenziali dell'account di gestione. Per abilitare la delega, devi considerare i prerequisiti elencati nella documentazione di IAM Identity Center. L'account amministratore delegato può eseguire la maggior parte delle attività di gestione di IAM Identity Center, ma con alcune restrizioni, elencate nella documentazione di IAM Identity Center. L'accesso all'account amministratore delegato per IAM Identity Center deve essere strettamente controllato.

Considerazioni di natura progettuale

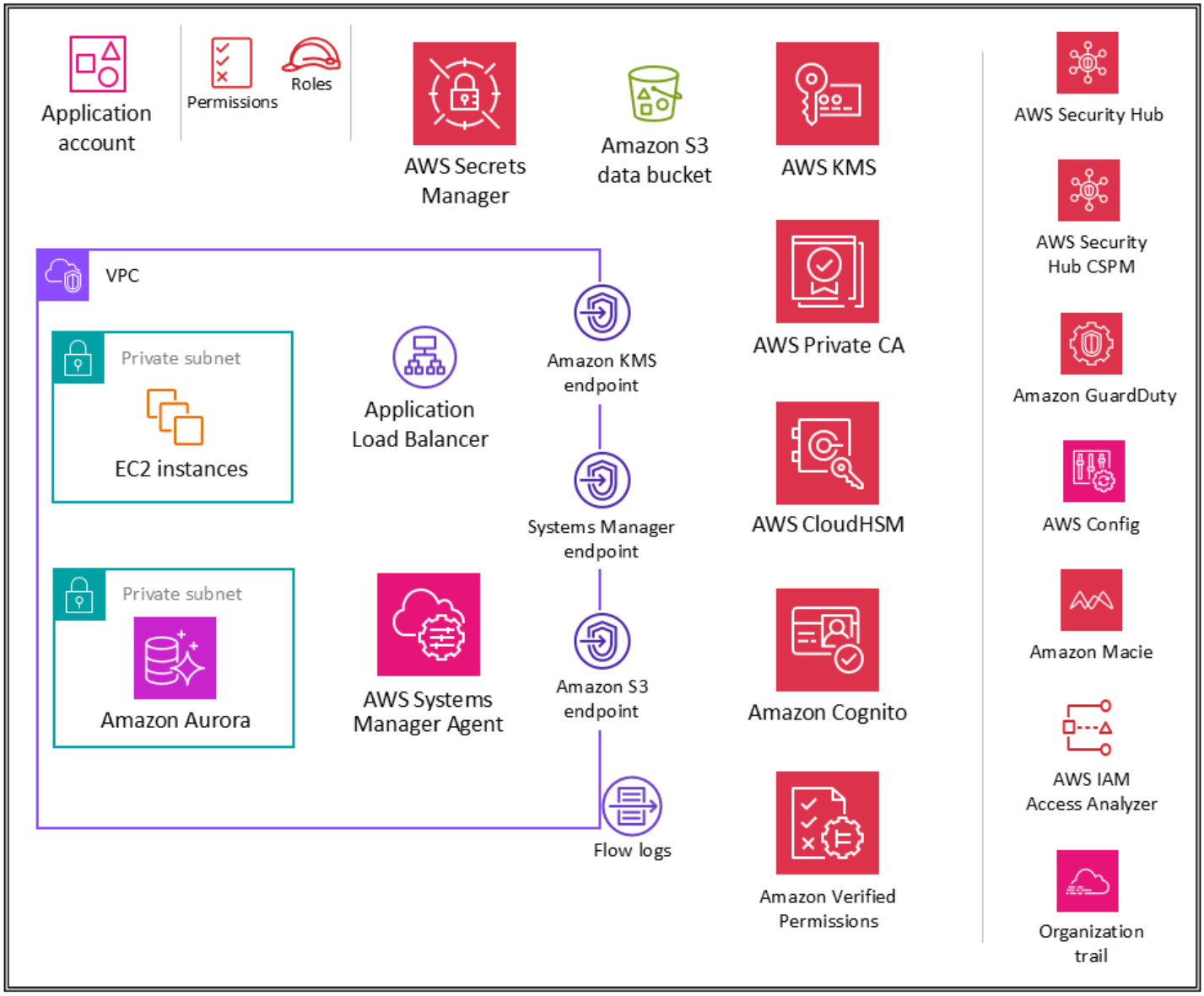
- Se decidi di cambiare la fonte di identità IAM Identity Center da qualsiasi altra fonte ad Active Directory o di cambiarla da Active Directory a qualsiasi altra fonte, la directory deve risiedere nell'account amministratore delegato di IAM Identity Center, se esistente, o deve essere nell'account di gestione.
- Puoi ospitare il tuo account AWS Managed Microsoft AD all'interno di un VPC dedicato in un altro account e quindi utilizzare AWS Resource Access Manager (AWS RAM) per condividere le sottoreti da quest'altro account all'account amministratore delegato. In questo modo, l' AWS Managed Microsoft AD istanza è controllata nell'account amministratore delegato, ma dal punto di vista della rete si comporta come se fosse distribuita nel VPC di un altro account. Ciò è utile quando si hanno più AWS Managed Microsoft AD istanze e si desidera distribuirle localmente dove viene eseguito il carico di lavoro, ma gestirle centralmente tramite un unico account.
- Se disponi di un team dedicato alle identità che svolge regolarmente attività di gestione delle identità e degli accessi o hai requisiti di sicurezza rigorosi per separare le funzioni di gestione delle identità dalle altre funzioni dei servizi condivisi, puoi ospitare un team dedicato alla Account AWS gestione delle identità. In questo scenario, designate questo account come amministratore delegato per IAM Identity Center e ospita anche la vostra AWS Managed Microsoft AD directory. Puoi raggiungere lo stesso livello di isolamento logico tra i carichi di lavoro di gestione delle identità e altri carichi di lavoro di servizi condivisi utilizzando autorizzazioni IAM granulari all'interno di un singolo account di servizio condiviso.
- Attualmente IAM Identity Center non fornisce supporto multiregionale. (Per abilitare IAM Identity Center in un'altra regione, devi prima eliminare la configurazione corrente di IAM Identity Center.) Inoltre, non supporta l'uso di diverse fonti di identità per diversi set di account né consente di delegare la gestione delle autorizzazioni a diverse parti dell'organizzazione (ovvero più amministratori delegati) o a diversi gruppi di amministratori.

Se hai bisogno di una di queste funzionalità, puoi utilizzare la federazione IAM per gestire le tue identità utente all'interno di un provider di identità (IdP) esterno e concedere a queste identità utente esterne l'autorizzazione a AWS utilizzare le risorse AWS del tuo account. Supporti IdPs IAM compatibili con OpenID Connect (OIDC) o SAML 2.0. Come best practice, usa la federazione SAML 2.0 con provider di identità di terze parti come Active Directory Federation Service (AD FS), Okta, Azure Active Directory (Azure AD) o Ping Identity per fornire funzionalità di single sign-on agli utenti per accedere o chiamare le operazioni API. Console di gestione AWS AWS Per ulteriori informazioni sulla federazione IAM e sui provider di identità, consulta Informazioni sulla federazione basata su SAML 2.0 nella documentazione IAM.

Workloads OU — Account dell'applicazione

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

Il diagramma seguente illustra i servizi AWS di sicurezza configurati nell'account dell'applicazione (insieme all'applicazione stessa).



L'account dell'applicazione ospita l'infrastruttura e i servizi principali per l'esecuzione e la manutenzione di un'applicazione aziendale. L'account dell'applicazione e l'unità organizzativa Workloads soddisfano alcuni obiettivi di sicurezza principali. Innanzitutto, crei un account separato per ogni applicazione per fornire limiti e controlli tra i carichi di lavoro in modo da evitare problemi legati alla combinazione di ruoli, autorizzazioni, dati e chiavi di crittografia. Desiderate fornire un contenitore di account separato in cui al team dell'applicazione possano essere concessi ampi diritti per gestire la propria infrastruttura senza influire sugli altri. Successivamente, si aggiunge un livello di protezione fornendo un meccanismo per il team addetto alle operazioni di sicurezza per monitorare e raccogliere i dati di sicurezza. Utilizza un percorso organizzativo e implementazioni locali di servizi di sicurezza degli account (Amazon GuardDuty,, AWS Security Hub CSPM Amazon AWS Config

EventBridge, IAM Access Analyzer), configurati e monitorati dal team di sicurezza. Infine, consentite alla vostra azienda di impostare i controlli a livello centrale. L'account dell'applicazione viene allineato alla struttura di sicurezza più ampia rendendolo membro dell'unità organizzativa Workloads tramite la quale eredita le autorizzazioni di servizio, i vincoli e le barriere appropriati.

> **Considerazione di natura progettuale**
>
> È probabile che nell'organizzazione siano presenti più di un'applicazione aziendale. L'unità organizzativa Workloads è progettata per ospitare la maggior parte dei carichi di lavoro specifici dell'azienda, inclusi ambienti di produzione e non di produzione. Questi carichi di lavoro possono essere una combinazione di applicazioni commerciali off-the-shelf (COTS) e applicazioni e servizi dati personalizzati sviluppati internamente. Esistono alcuni modelli per organizzare le diverse applicazioni aziendali insieme ai relativi ambienti di sviluppo. Uno schema prevede l'utilizzo di più elementi secondari in OUs base all'ambiente di sviluppo, ad esempio produzione, gestione temporanea, test e sviluppo, e l'utilizzo di elementi secondari Account AWS separati tra OUs quelli relativi alle diverse applicazioni. Un altro modello comune consiste nell'avere figli separati OUs per applicazione e quindi utilizzare elementi secondari separati Account AWS per i singoli ambienti di sviluppo. L'esatta struttura dell'unità organizzativa e degli account dipende dal design dell'applicazione e dai team che gestiscono tali applicazioni. Considerate i controlli di sicurezza che desiderate applicare, siano essi specifici dell'ambiente o dell'applicazione, perché è più facile implementare tali controlli così come sono. SCPs OUs Per ulteriori considerazioni sull'organizzazione orientata al carico di lavoro OUs, consulta la sezione Applicazione OUs del white paper Organizzazione dell'ambiente utilizzando più account. AWS AWS

Applicazione VPC

Il cloud privato virtuale (VPC) nell'account dell'applicazione richiede sia l'accesso in entrata (per i semplici servizi Web che si stanno modellando) sia l'accesso in uscita (per le esigenze o le esigenze delle applicazioni). Servizio AWS Per impostazione predefinita, le risorse all'interno di un VPC sono instradabili tra loro. Esistono due sottoreti private: una per ospitare le EC2 istanze (livello applicazione) e l'altra per Amazon Aurora (livello database). La segmentazione della rete tra diversi livelli, come il livello dell'applicazione e il livello del database, viene eseguita tramite gruppi di sicurezza VPC, che limitano il traffico a livello di istanza. Per garantire la resilienza, il carico di lavoro si estende su due o più zone di disponibilità e utilizza due sottoreti per zona.

Considerazione di natura progettuale

È possibile utilizzare Traffic Mirroring per copiare il traffico di rete da un'interfaccia di rete elastica di EC2 istanze. È quindi possibile inviare il traffico ai dispositivi di out-of-band sicurezza e monitoraggio per l'ispezione dei contenuti, il monitoraggio delle minacce o la risoluzione dei problemi. Ad esempio, potresti voler monitorare il traffico che esce dal tuo VPC o il traffico la cui fonte è esterna al tuo VPC. In questo caso, rispecchierai tutto il traffico ad eccezione del traffico che passa all'interno del tuo VPC e lo invierai a un singolo dispositivo di monitoraggio. I log di flusso di Amazon VPC non acquisiscono traffico speculare; in genere acquisiscono informazioni solo dalle intestazioni dei pacchetti. Traffic Mirroring fornisce una visione più approfondita del traffico di rete consentendoti di analizzare il contenuto effettivo del traffico, incluso il payload. Abilita il mirroring del traffico solo per l'interfaccia di rete elastica delle EC2 istanze che potrebbero funzionare come parte di carichi di lavoro sensibili o per le quali prevedi di aver bisogno di una diagnostica dettagliata in caso di problemi.

Endpoint VPC

Gli endpoint VPC forniscono un altro livello di controllo della sicurezza oltre a scalabilità e affidabilità. Utilizzali per connettere il VPC dell'applicazione ad altri. Servizi AWS(Nell'account Application, AWS SRA utilizza endpoint VPC per AWS KMS e AWS Systems Manager Amazon S3.) Gli endpoint sono dispositivi virtuali. Sono componenti VPC con scalabilità orizzontale, ridondanza e disponibilità elevata. Consentono la comunicazione tra istanze del VPC e servizi senza comportare rischi di disponibilità o vincoli di larghezza di banda sul traffico di rete. Puoi utilizzare un endpoint VPC per connettere privatamente il tuo VPC a servizi endpoint VPC supportati Servizi AWS e forniti AWS PrivateLink da senza richiedere un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze nel tuo VPC non richiedono indirizzi IP pubblici per comunicare con altri. Servizi AWS Il traffico tra il tuo VPC e l'altro Servizio AWS non esce dalla rete Amazon.

Un altro vantaggio dell'utilizzo degli endpoint VPC è l'abilitazione della configurazione delle policy degli endpoint. Una policy endpoint VPC è una policy della risorsa IAM che viene collegata a un endpoint durante la creazione o la modifica dell'endpoint. Se non alleghi una policy IAM quando crei un endpoint, ti AWS allega una policy IAM predefinita che consente l'accesso completo al servizio. Una policy endpoint non esclude né sostituisce policy dell'utente IAM o policy specifiche del servizio (ad esempio policy di un bucket S3). Si tratta di una policy IAM separata per il controllo dell'accesso

dall'endpoint al servizio specificato. In questo modo, aggiunge un altro livello di controllo su quali AWS mandanti possono comunicare con risorse o servizi.

Amazon EC2

Le EC2 istanze Amazon che compongono la nostra applicazione utilizzano la versione 2 di Instance Metadata Service (). IMDSv2 IMDSv2 aggiunge protezioni per quattro tipi di vulnerabilità che potrebbero essere utilizzate per tentare di accedere all'IMDS: firewall delle applicazioni dei siti Web, proxy inversi aperti, vulnerabilità SSRF (server-side request forgery), firewall open layer 3 e. NATs Per ulteriori informazioni, consulta il post sul blog Aggiungi una difesa approfondita contro firewall aperti, proxy inversi e vulnerabilità SSRF con miglioramenti all'Instance Metadata Service. EC2

Utilizza elementi separati VPCs (come sottoinsieme dei confini dell'account) per isolare l'infrastruttura in base ai segmenti del carico di lavoro. Utilizza sottoreti per isolare i livelli dell'applicazione (ad esempio, web, applicazione e database) all'interno di un singolo VPC. Utilizza sottoreti private per le istanze se non devono essere accessibili direttamente da Internet. Per chiamare l' EC2API Amazon dalla tua sottorete privata senza utilizzare un gateway Internet, usa AWS PrivateLink. Limita l'accesso alle tue istanze utilizzando gruppi di sicurezza. Usa VPC Flow Logs per monitorare il traffico che raggiunge le tue istanze. Usa Session Manager, una funzionalità di AWS Systems Manager, per accedere alle istanze da remoto invece di aprire porte SSH in entrata e gestire le chiavi SSH. Usa volumi Amazon Elastic Block Store (Amazon EBS) separati per il sistema operativo e i tuoi dati. Puoi configurare il tuo Account AWS per applicare la crittografia dei nuovi volumi EBS e delle copie di snapshot che crei.

> **Esempio di implementazione**
>
> La libreria di codici AWS SRA fornisce un'implementazione di esempio della crittografia Amazon EBS predefinita in Amazon. EC2 Dimostra come abilitare la crittografia Amazon EBS predefinita a livello di account all'interno di ciascun account Account AWS e Regione AWS all'interno dell'organizzazione. AWS

AWS Enclavi Nitro

AWS Nitro Enclaves è una EC2 funzionalità di Amazon che consente di creare ambienti di esecuzione isolati, chiamati enclavi, a partire dalle istanze. EC2 Le enclave sono macchine virtuali separate, rinforzate e altamente vincolate. La CPU e la memoria di una singola EC2 istanza principale sono partizionate in enclavi isolate. Ogni enclave esegue un kernel indipendente. Le

enclavi forniscono solo una connettività socket locale sicura con l'istanza principale. Non dispongono di archiviazione persistente, accesso interattivo o reti esterne. Gli utenti non possono accedere a un'enclave tramite SSH e i processi, le applicazioni o gli utenti (root o amministratore) dell'istanza principale non possono accedere ai dati e alle applicazioni all'interno dell'enclave. È possibile proteggere i dati più sensibili, come le informazioni di identificazione personale (PII), i dati sanitari, finanziari e sulla proprietà intellettuale, all'interno delle istanze. EC2 Nitro Enclaves ti consente di concentrarti sulla tua applicazione anziché preoccuparti dell'integrazione con servizi esterni. Nitro Enclaves include l'attestazione crittografica per il software in modo da avere la certezza che sia in esecuzione solo il codice autorizzato e l'integrazione con la in modo che solo le enclavi possano accedere a materiale sensibile. AWS KMS Questo aiuta a ridurre la superficie di attacco per le applicazioni di elaborazione dati più sensibili. L'utilizzo di Nitro Enclaves non comporta costi aggiuntivi.

L'attestazione crittografica è un processo utilizzato per dimostrare l'identità di un'enclave. Il processo di attestazione viene eseguito tramite l'Hypervisor Nitro, che produce un documento di attestazione firmato per l'enclave per dimostrare la sua identità a un'altra terza parte o servizio. I documenti di attestazione contengono dettagli chiave dell'enclave, come la chiave pubblica dell'enclave, gli hash dell'immagine e delle applicazioni dell'enclave e altro ancora.

Con AWS Certificate Manager (ACM) for Nitro Enclaves, puoi utilizzare certificati pubblici e privati. SSL/TLS certificates with your web applications and web servers running on EC2 instances with Nitro Enclaves. SSL/TLS certificates are used to secure network communications and to establish the identity of websites over the internet and resources on private networks. ACM for Nitro Enclaves removes the time-consuming and error-prone manual process of purchasing, uploading, and renewing SSL/TLS ACM for Nitro Enclaves crea chiavi private sicure, distribuisce il certificato e la relativa chiave privata nell'enclave e gestisce i rinnovi dei certificati. Con ACM for Nitro Enclaves, la chiave privata del certificato rimane isolata nell'enclave, il che impedisce all'istanza e ai suoi utenti di accedervi. Per ulteriori informazioni, consulta Nitro Enclaves nella documentazione AWS Certificate Manager di Nitro Enclaves.

Application Load Balancer

Gli Application Load Balancer distribuiscono il traffico delle applicazioni in entrata su più destinazioni, ad esempio istanze, in più zone di disponibilità. EC2 Nell' AWS SRA, il gruppo target per il load balancer sono le istanze dell'applicazione. EC2 L' AWS SRA utilizza listener HTTPS per garantire che il canale di comunicazione sia crittografato. L'Application Load Balancer utilizza un certificato server per interrompere la connessione front-end e quindi per decrittografare le richieste dei client prima di inviarle alle destinazioni.

AWS Certificate Manager (ACM) si integra nativamente con Application Load Balancers e AWS SRA utilizza ACM per generare e gestire i certificati pubblici X.509 (server TLS) necessari. È possibile applicare TLS 1.2 e cifrari avanzati per le connessioni front-end tramite la policy di sicurezza Application Load Balancer. Per ulteriori informazioni, consulta la Guida per l'utente di Elastic Load Balancing.

Considerazioni di natura progettuale

- Per scenari comuni come applicazioni strettamente interne che richiedono un certificato TLS privato su Application Load Balancer, puoi utilizzare ACM all'interno di questo account per generare un certificato privato da. AWS Private CANell' AWS SRA, la CA principale privata ACM è ospitata nell'account Security Tooling e può essere condivisa con l'intera AWS organizzazione o con certificati di entità finale specifici Account AWS per l'emissione, come descritto in precedenza nella sezione Account Security Tooling.
- Per i certificati pubblici, puoi utilizzare ACM per generare tali certificati e gestirli, inclusa la rotazione automatica. In alternativa, puoi generare i tuoi certificati utilizzando SSL/TLS strumenti per creare una richiesta di firma del certificato (CSR), far firmare la CSR da un'autorità di certificazione (CA) per produrre un certificato, quindi importare il certificato in ACM o caricare il certificato su IAM per utilizzarlo con Application Load Balancer. Se importi un certificato in ACM, devi monitorare la data di scadenza del certificato e rinnovarlo prima della scadenza.
- Per ulteriori livelli di difesa, puoi implementare AWS WAF policy per proteggere l'Application Load Balancer. La presenza di policy edge, policy applicative e persino livelli di applicazione delle policy privati o interni aumenta la visibilità delle richieste di comunicazione e garantisce un'applicazione unificata delle policy. Per ulteriori informazioni, consulta il post sul blog Deploying defense in depth using Regole gestite da AWS for. AWS WAF

AWS Private CA

AWS Autorità di certificazione privata(AWS Private CA) viene utilizzato nell'account dell'applicazione per generare certificati privati da utilizzare con un Application Load Balancer. È uno scenario comune che Application Load Balancer fornisca contenuti sicuri tramite TLS. Ciò richiede l'installazione di certificati TLS sull'Application Load Balancer. Per le applicazioni strettamente interne, i certificati TLS privati possono fornire un canale sicuro.

In AWS SRA, AWS Private CA è ospitato nell'account Security Tooling ed è condiviso con l'account dell'Applicazione utilizzando. AWS RAM Ciò consente agli sviluppatori di un account dell'Applicazione di richiedere un certificato da una CA privata condivisa. La CAs condivisione all'interno o all'interno dell'organizzazione Account AWS aiuta a ridurre i costi e la complessità legati alla creazione e alla gestione dei duplicati CAs in tutta l'organizzazione Account AWS. Quando utilizzi ACM per emettere certificati privati da una CA condivisa, il certificato viene generato localmente nell'account richiedente e ACM fornisce la gestione e il rinnovo completi del ciclo di vita.

Amazon Inspector

L' AWS SRA utilizza Amazon Inspector per rilevare e EC2 scansionare automaticamente le istanze e le immagini dei container che risiedono in Amazon Elastic Container Registry (Amazon ECR) alla ricerca di vulnerabilità del software ed esposizione involontaria della rete.

Amazon Inspector viene inserito nell'account Application, poiché fornisce servizi di gestione delle vulnerabilità alle EC2 istanze di questo account. Inoltre, Amazon Inspector segnala percorsi di rete indesiderati da EC2 e verso le istanze.

Amazon Inspector negli account dei membri è gestito centralmente dall'account amministratore delegato. In AWS SRA, l'account Security Tooling è l'account amministratore delegato. L'account amministratore delegato può gestire i risultati, i dati e alcune impostazioni per i membri dell'organizzazione. Ciò include la visualizzazione dei dettagli aggregati dei risultati per tutti gli account dei membri, l'attivazione o la disabilitazione delle scansioni per gli account dei membri e la revisione delle risorse analizzate all'interno dell'organizzazione. AWS

> **Considerazione di natura progettuale**
>
> Puoi utilizzare Patch Manager, una funzionalità di AWS Systems Manager, per attivare patch su richiesta per correggere vulnerabilità di sicurezza zero-day di Amazon Inspector o altre vulnerabilità di sicurezza critiche. Patch Manager ti aiuta a correggere queste vulnerabilità senza dover attendere la normale pianificazione delle patch. La correzione viene eseguita utilizzando il runbook Systems Manager Automation. Per ulteriori informazioni, consulta la serie di blog in due parti Automatizzare la gestione e la correzione delle vulnerabilità utilizzando Amazon AWS Inspector e. AWS Systems Manager

AWS Systems Manager

AWS Systems Managerè uno strumento Servizio AWS che puoi utilizzare per visualizzare i dati operativi provenienti da più risorse Servizi AWS e automatizzare le attività operative tra le tue risorse. AWS Con i flussi di lavoro e i runbook di approvazione automatizzati, puoi lavorare per ridurre gli errori umani e semplificare le attività di manutenzione e distribuzione delle risorse. AWS

Oltre a queste funzionalità di automazione generali, Systems Manager supporta una serie di funzionalità di sicurezza preventive, investigative e reattive. AWS Systems Manager Agent (SSM Agent) è un software Amazon che può essere installato e configurato su un' EC2 istanza, un server locale o una macchina virtuale (VM). SSM Agent consente a Systems Manager di aggiornare, gestire e configurare tali risorse. Systems Manager ti aiuta a mantenere la sicurezza e la conformità scansionando queste istanze gestite e segnalando (o adottando azioni correttive) su eventuali violazioni rilevate nelle patch, nella configurazione e nelle politiche personalizzate.

L' AWS SRA utilizza Session Manager, una funzionalità di Systems Manager, per fornire una shell interattiva basata su browser e un'esperienza CLI. Ciò fornisce una gestione delle istanze sicura e verificabile senza la necessità di aprire porte in ingresso, mantenere host bastion o gestire chiavi SSH. L' AWS SRA utilizza Patch Manager, una funzionalità di Systems Manager, per applicare patch alle EC2 istanze sia per i sistemi operativi che per le applicazioni.

L' AWS SRA utilizza anche Automation, una funzionalità di Systems Manager, per semplificare le attività comuni di manutenzione e distribuzione delle EC2 istanze Amazon e di altre AWS risorse. Il servizio di automazione consente di semplificare le attività IT più comuni, ad esempio la modifica dello stato di una o più nodi (utilizzando un'automazione di approvazione) e la gestione dello stato dei nodi in base a una pianificazione. Systems Manager comprende caratteristiche che supportano la gestione di grandi gruppi di istanze mediante l'uso di tag e controlli di velocità che semplificano l'implementazione delle modifiche in base ai limiti da te definiti. L'automazione offre automazioni con un solo clic per semplificare attività complesse come la creazione di Amazon Machine Images dorate (AMIs) e il ripristino di istanze irraggiungibili. EC2 Inoltre, puoi migliorare la sicurezza operativa dando ai ruoli IAM l'accesso a runbook specifici per eseguire determinate funzioni, senza concedere direttamente le autorizzazioni a tali ruoli. Ad esempio, se desideri che un ruolo IAM disponga delle autorizzazioni per riavviare EC2 istanze specifiche dopo gli aggiornamenti delle patch, ma non vuoi concedere l'autorizzazione direttamente a quel ruolo, puoi invece creare un runbook di automazione e concedere al ruolo le autorizzazioni per eseguire solo il runbook.

Considerazioni di natura progettuale

- Systems Manager si affida ai metadati delle EC2 istanze per funzionare correttamente. Systems Manager può accedere ai metadati dell'istanza utilizzando la versione 1 o la versione 2 di Instance Metadata Service (IMDSv1 and IMDSv2).
- SSM Agent deve comunicare con diverse Servizi AWS risorse come Amazon EC2 messages, Systems Manager e Amazon S3. Affinché questa comunicazione avvenga, la sottorete richiede la connettività Internet in uscita o il provisioning di endpoint VPC appropriati. L' AWS SRA utilizza gli endpoint VPC per l'agente SSM per stabilire percorsi di rete privati verso vari. Servizi AWS
- L'utilizzo dell'automazione consente di condividere le best practice con tutta l'organizzazione. È possibile creare best practice per la gestione delle risorse nei runbook e condividere i runbook tra e gruppi. Regioni AWS Puoi anche limitare i valori consentiti per i parametri del runbook. In questi casi d'uso, potrebbe essere necessario creare runbook di automazione in un account centrale come Security Tooling o Shared Services e condividerli con il resto dell'organizzazione. AWS I casi d'uso più comuni includono la capacità di implementare centralmente patch e aggiornamenti di sicurezza, rimediare alla deriva dalle configurazioni VPC o dalle policy dei bucket S3 e gestire le istanze su larga scala. EC2 Per i dettagli sull'implementazione, vedere la documentazione di Systems Manager.

Amazon Aurora

Nell' AWS SRA, Amazon Aurora e Amazon S3 costituiscono il livello logico dei dati. Aurora è un motore di database relazionale completamente gestito compatibile con MySQL e PostgreSQL. Un'applicazione in esecuzione sulle EC2 istanze comunica con Aurora e Amazon S3 in base alle esigenze. Aurora è configurata con un cluster di database all'interno di un sottogruppo di database.

Considerazione di natura progettuale

Come in molti servizi di database, la sicurezza per Aurora è gestita su tre livelli. Per controllare chi può eseguire azioni di gestione di Amazon Relational Database Service (Amazon RDS) su cluster e istanze DB Aurora, utilizzi IAM. Per controllare quali dispositivi e EC2 istanze possono aprire connessioni all'endpoint e alla porta del cluster dell'istanza DB per i cluster Aurora DB in un VPC, si utilizza un gruppo di sicurezza VPC. Per autenticare gli accessi e le autorizzazioni per un cluster Aurora DB, puoi adottare lo stesso approccio

di un'istanza DB autonoma di MySQL o PostgreSQL oppure puoi utilizzare l'autenticazione del database IAM per Aurora MySQL Compatible Edition. Con quest'ultimo approccio, ti autentichi nel tuo cluster DB Aurora compatibile con MySQL utilizzando un ruolo IAM e un token di autenticazione.

Simple Storage Service (Amazon S3)

Amazon S3 è un servizio di storage di oggetti che offre scalabilità, disponibilità dei dati, sicurezza e prestazioni all'avanguardia nel settore. È la spina dorsale dei dati di molte applicazioni basate su AWS di essa e autorizzazioni e controlli di sicurezza appropriati sono fondamentali per proteggere i dati sensibili. Per le best practice di sicurezza consigliate per Amazon S3, consulta la documentazione, i talk tecnici online e approfondimenti nei post del blog. La best practice più importante consiste nel bloccare l'accesso eccessivamente permissivo (in particolare l'accesso pubblico) ai bucket S3.

AWS KMS

L' AWS SRA illustra il modello di distribuzione consigliato per la gestione delle chiavi, in cui le chiavi AWS KMS key risiedono all'interno della stessa risorsa da crittografare. Account AWS Per questo motivo, AWS KMS viene utilizzato nell'account dell'applicazione oltre ad essere incluso nell'account Security Tooling. Nell'account dell'applicazione, AWS KMS viene utilizzato per gestire le chiavi specifiche delle risorse dell'applicazione. È possibile implementare una separazione delle funzioni utilizzando politiche chiave per concedere le autorizzazioni di utilizzo delle chiavi ai ruoli delle applicazioni locali e per limitare le autorizzazioni di gestione e monitoraggio ai custodi chiave.

Considerazione di natura progettuale

In un modello distribuito, la responsabilità AWS KMS chiave della gestione spetta al team dell'applicazione. Tuttavia, il team di sicurezza centrale può essere responsabile della governance e del monitoraggio di importanti eventi crittografici come i seguenti:

- Il materiale chiave importato in una chiave KMS si avvicina alla data di scadenza.
- Il materiale chiave di una chiave KMS è stato ruotato automaticamente.
- La chiave AKMS è stata eliminata.
- C'è un alto tasso di errori di decrittografia.

AWS CloudHSM

AWS CloudHSMfornisce moduli di sicurezza hardware gestiti (HSMs) in. Cloud AWS Consente di generare e utilizzare le proprie chiavi di crittografia AWS utilizzando lo standard FIPS 140-2 di livello 3 convalidato a HSMs cui è possibile controllare l'accesso. È possibile utilizzarlo AWS CloudHSM per eseguire l'offload dell' SSL/TLS elaborazione per i server Web. Ciò riduce il carico sul server Web e fornisce una maggiore sicurezza memorizzando la chiave privata del server Web. AWS CloudHSM Allo stesso modo, puoi implementare un HSM dal VPC AWS CloudHSM in entrata nell'account di rete per archiviare le tue chiavi private e firmare le richieste di certificato se devi agire come autorità di certificazione emittente.

> Considerazione di natura progettuale
>
> Se hai un requisito rigoroso per FIPS 140-2 livello 3, puoi anche scegliere di configurare l'utilizzo del AWS CloudHSM cluster come archivio AWS KMS di chiavi personalizzato anziché utilizzare l'archivio di chiavi KMS nativo. In questo modo, trarrai vantaggio dall'integrazione AWS KMS e Servizi AWS dalla crittografia dei tuoi dati, pur essendo responsabile della protezione delle tue chiavi HSMs KMS. Ciò combina il sistema single-tenant HSMs sotto il tuo controllo con la facilità d'uso e l'integrazione di. AWS KMS Per gestire l' AWS CloudHSM infrastruttura, è necessario utilizzare un'infrastruttura a chiave pubblica (PKI) e disporre di un team con esperienza nella gestione. HSMs

Gestione dei segreti AWS

Gestione dei segreti AWSti aiuta a proteggere le credenziali (segreti) di cui hai bisogno per accedere alle tue applicazioni, servizi e risorse IT. Il servizio consente di ruotare, gestire e recuperare in modo efficiente le credenziali del database, le chiavi API e altri segreti durante tutto il loro ciclo di vita. Puoi sostituire le credenziali codificate nel codice con una chiamata API a Secrets Manager per recuperare il segreto a livello di codice. Questo aiuta a garantire che il segreto non possa essere compromesso da qualcuno che sta esaminando il codice, perché il segreto non esiste più nel codice. Inoltre, Secrets Manager consente di spostare le applicazioni tra ambienti (sviluppo, preproduzione, produzione). Invece di modificare il codice, potete assicurarvi che nell'ambiente sia disponibile un segreto denominato e referenziato in modo appropriato. Ciò favorisce la coerenza e la riutilizzabilità del codice applicativo in diversi ambienti, richiedendo al contempo un minor numero di modifiche e interazioni umane dopo il test del codice.

Con Secrets Manager, puoi gestire l'accesso ai segreti utilizzando policy IAM granulari e politiche basate sulle risorse. Puoi contribuire a proteggere i segreti crittografandoli con chiavi di crittografia che gestisci utilizzando. AWS KMS Secrets Manager si integra anche con i servizi AWS di registrazione e monitoraggio per il controllo centralizzato.

Secrets Manager utilizza la crittografia a busta con AWS KMS keys chiavi dati per proteggere ogni valore segreto. Quando crei un segreto, puoi scegliere qualsiasi chiave simmetrica gestita dal cliente nella regione Account AWS and oppure puoi utilizzare la chiave AWS gestita per Secrets Manager.

Come best practice, puoi monitorare i tuoi segreti per registrare eventuali modifiche. Questo vi aiuta a garantire che eventuali utilizzi o modifiche imprevisti possano essere esaminati. Le modifiche indesiderate possono essere annullate. Secrets Manager attualmente ne supporta due Servizi AWS che consentono di monitorare l'organizzazione e l'attività: AWS CloudTrail e AWS Config. CloudTrail acquisisce tutte le chiamate API per Secrets Manager come eventi, incluse le chiamate dalla console Secrets Manager e le chiamate di codice a Secrets Manager APIs. Inoltre, CloudTrail acquisisce altri eventi correlati (non API) che potrebbero avere un impatto sulla sicurezza o sulla conformità o che potrebbero aiutarti a risolvere problemi operativi. Account AWS Questi includono alcuni eventi di rotazione dei segreti e l'eliminazione di versioni segrete. AWS Config può fornire controlli investigativi tracciando e monitorando le modifiche ai segreti in Secrets Manager. Queste modifiche includono la descrizione di un segreto, la configurazione di rotazione, i tag e la relazione con altre AWS fonti, come la chiave di crittografia KMS o AWS Lambda le funzioni utilizzate per la rotazione segreta. Puoi anche configurare Amazon EventBridge, che riceve notifiche di modifica della configurazione e della conformità AWS Config, per indirizzare particolari eventi segreti per azioni di notifica o correzione.

In AWS SRA, Secrets Manager si trova nell'account dell'applicazione per supportare i casi d'uso delle applicazioni locali e per gestire i segreti vicini al loro utilizzo. Qui, un profilo di istanza è allegato alle EC2 istanze nell'account dell'applicazione. È quindi possibile configurare segreti separati in Secrets Manager per consentire a quel profilo di istanza di recuperare segreti, ad esempio per unirsi al dominio Active Directory o LDAP appropriato e accedere al database Aurora. Secrets Manager si integra con Amazon RDS per gestire le credenziali utente quando crei, modifichi o ripristini un'istanza database Amazon RDS o un cluster DB Multi-AZ. Ciò consente di gestire la creazione e la rotazione delle chiavi e sostituisce le credenziali codificate nel codice con chiamate API programmatiche a Secrets Manager.

> **Considerazione di natura progettuale**
>
> In generale, configura e gestisci Secrets Manager nell'account più vicino a dove verranno utilizzati i segreti. Questo approccio sfrutta la conoscenza locale del caso d'uso e offre

velocità e flessibilità ai team di sviluppo delle applicazioni. Per informazioni strettamente controllate che potrebbero richiedere un ulteriore livello di controllo, i segreti possono essere gestiti centralmente da Secrets Manager nell'account Security Tooling.

Amazon Cognito

Amazon Cognito ti consente di aggiungere la registrazione, l'accesso e il controllo degli accessi degli utenti alle tue app Web e mobili in modo rapido ed efficiente. Amazon Cognito è scalabile fino a milioni di utenti e supporta l'accesso con provider di identità social, come Apple, Facebook, Google e Amazon, e provider di identità aziendali tramite SAML 2.0 e OpenID Connect. I due componenti principali di Amazon Cognito sono i pool di utenti e i pool di identità. I pool di utenti sono directory di utenti che forniscono opzioni di registrazione e accesso per gli utenti dell'applicazione. I pool di identità consentono di concedere ai propri utenti l'accesso ad altri. Servizi AWSÈ possibile usare i pool di identità e i bacini d'utenza separatamente o insieme. Per scenari di utilizzo comuni, consulta la documentazione di Amazon Cognito.

Amazon Cognito offre un'interfaccia utente integrata e personalizzabile per la registrazione e l'accesso degli utenti. Puoi usare Android, iOS e Amazon Cognito JavaScript SDKs per aggiungere pagine di registrazione e accesso degli utenti alle tue app. Amazon Cognito Sync è una Servizio AWS libreria client che consente la sincronizzazione tra dispositivi dei dati utente relativi alle applicazioni.

Amazon Cognito supporta l'autenticazione e la crittografia a più fattori dei dati inattivi e dei dati in transito. I pool di utenti di Amazon Cognito forniscono funzionalità di sicurezza avanzate per proteggere l'accesso agli account utente nell'applicazione. Queste funzionalità di sicurezza avanzate forniscono autenticazione adattiva basata sul rischio e protezione dall'uso di credenziali compromesse.

Considerazioni di natura progettuale

- È possibile creare una AWS Lambda funzione e quindi attivarla durante le operazioni del pool di utenti come l'iscrizione, la conferma e l'accesso (autenticazione) degli utenti con un trigger Lambda. Puoi aggiungere i problemi di autenticazione, migrare gli utenti e personalizzare i messaggi di verifica. Per le operazioni e il flusso di utenti comuni, consulta la documentazione di Amazon Cognito. Amazon Cognito chiama le funzioni Lambda in modo sincrono.

- Puoi utilizzare i pool di utenti di Amazon Cognito per proteggere piccole applicazioni multi-tenant. Un caso d'uso comune della progettazione multi-tenant consiste nell'esecuzione di carichi di lavoro per supportare il test di più versioni di un'applicazione. La progettazione multi-tenant è utile anche per testare una singola applicazione con diversi set di dati che consente l'uso completo delle risorse del cluster. Tuttavia, assicurati che il numero di inquilini e il volume previsto siano in linea con le relative quote del servizio Amazon Cognito. Queste quote vengono condivise tra tutti i tenant dell'applicazione.

Autorizzazioni verificate da Amazon

Amazon Verified Permissions è un servizio scalabile di gestione delle autorizzazioni e di autorizzazione granulare per le applicazioni che crei. Gli sviluppatori e gli amministratori possono utilizzare Cedar, un linguaggio di policy open source creato appositamente e incentrato sulla sicurezza, con ruoli e attributi per definire controlli di accesso più granulari, sensibili al contesto e basati su policy. Gli sviluppatori possono creare applicazioni più sicure più rapidamente esternalizzando le autorizzazioni e centralizzando la gestione e l'amministrazione delle policy. Le autorizzazioni verificate includono definizioni di schemi, formulazioni di policy, grammatica e ragionamento automatico che si estendono a milioni di autorizzazioni, in modo da poter applicare i principi di negazione predefinita e privilegio minimo. Il servizio include anche uno strumento di simulazione di valutazione per aiutarvi a testare le vostre decisioni di autorizzazione e le politiche relative agli autori. Queste funzionalità facilitano l'implementazione di un modello di autorizzazione approfondito e granulare per supportare gli obiettivi zero-trust. Verified Permissions centralizza le autorizzazioni in un archivio di policy e aiuta gli sviluppatori a utilizzare tali autorizzazioni per autorizzare le azioni degli utenti all'interno delle loro applicazioni.

È possibile connettere l'applicazione al servizio tramite l'API per autorizzare le richieste di accesso degli utenti. Per ogni richiesta di autorizzazione, il servizio recupera le politiche pertinenti e le valuta per determinare se un utente è autorizzato a intraprendere un'azione su una risorsa, in base a input di contesto quali utenti, ruoli, appartenenza al gruppo e attributi. È possibile configurare e connettere le autorizzazioni verificate a cui inviare i registri di gestione e autorizzazione delle politiche. AWS CloudTrail Se utilizzi Amazon Cognito come archivio di identità, puoi effettuare l'integrazione con Autorizzazioni verificate e utilizzare l'ID e i token di accesso che Amazon Cognito restituisce nelle decisioni di autorizzazione delle tue applicazioni. Fornisci token Amazon Cognito a Verified Permissions, che utilizza gli attributi contenuti nei token per rappresentare il principale e identificare i diritti del principale. Per ulteriori informazioni su questa integrazione, consulta il post del

AWS blog Semplificazione dell'autorizzazione granulare con Amazon Verified Permissions e Amazon Cognito.

Verified Permissions ti aiuta a definire il controllo degli accessi basato su policy (PBAC). PBAC è un modello di controllo degli accessi che utilizza le autorizzazioni espresse sotto forma di policy per determinare chi può accedere a quali risorse in un'applicazione. PBAC unisce il controllo degli accessi basato sui ruoli (RBAC) e il controllo degli accessi basato sugli attributi (ABAC), dando vita a un modello di controllo degli accessi più potente e flessibile. Per ulteriori informazioni su PBAC e su come progettare un modello di autorizzazione utilizzando Autorizzazioni verificate, consulta il post del AWS blog Controllo degli accessi basato su policy nello sviluppo di applicazioni con Amazon Verified Permissions.

Nella AWS SRA, Verified Permissions si trova nell'account dell'Applicazione per supportare la gestione delle autorizzazioni per le applicazioni attraverso la sua integrazione con Amazon Cognito.

Difesa a più livelli

L'account Application offre l'opportunità di illustrare i principi di difesa a più livelli che consentono. AWS Considerate la sicurezza delle EC2 istanze che costituiscono il nucleo di una semplice applicazione di esempio rappresentata nell' AWS SRA e vedrete come Servizi AWS cooperare in una difesa a più livelli. Questo approccio è in linea con la visione strutturale dei servizi di AWS sicurezza, come descritto nella sezione Applica i servizi di sicurezza in tutta l' AWS organizzazione precedente di questa guida.

- Lo strato più interno sono le istanze. EC2 Come accennato in precedenza, EC2 le istanze includono molte funzionalità di sicurezza native per impostazione predefinita o come opzioni. Alcuni esempi includono IMDSv2il sistema Nitro e la crittografia dello storage Amazon EBS.
- Il secondo livello di protezione si concentra sul sistema operativo e sul software in esecuzione sulle EC2 istanze. Servizi come Amazon Inspector ti AWS Systems Managerconsentono di monitorare, generare report e intraprendere azioni correttive su queste configurazioni. Amazon Inspector monitora il tuo software alla ricerca di vulnerabilità e Systems Manager ti aiuta a mantenere la sicurezza e la conformità scansionando le istanze gestite per verificarne lo stato di patch e configurazione, quindi segnalando e adottando le azioni correttive da te specificate.
- Le istanze e il software in esecuzione su queste istanze sono integrate nell'infrastruttura di rete. AWS Oltre a utilizzare le funzionalità di sicurezza di Amazon VPC, AWS SRA utilizza anche endpoint VPC per fornire connettività privata tra il VPC e il supporto e per fornire un meccanismo per posizionare le Servizi AWS politiche di accesso ai confini della rete.

- L'attività e la configurazione delle EC2 istanze, del software, della rete e dei ruoli e delle risorse IAM sono ulteriormente monitorate da servizi Account AWS focalizzati come AWS Security Hub Amazon AWS Security Hub CSPM, GuardDuty AWS CloudTrail AWS Config, IAM Access Analyzer e Amazon Macie.
- Infine, oltre all'account Application, AWS RAM aiuta a controllare quali risorse sono condivise con altri account e le policy di controllo dei servizi IAM ti aiutano a far rispettare autorizzazioni coerenti in tutta l'organizzazione. AWS

AI/ML per la sicurezza

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

L'intelligenza artificiale e l'apprendimento automatico (AI/ML) is transforming businesses. AI/MLsono al centro dell'attenzione di Amazon da oltre 20 anni) e molte delle funzionalità utilizzate dai clienti AWS, compresi i servizi di sicurezza, sono basate sull'AI/ML. Questo crea un valore integrato e differenziato, perché è possibile sviluppare in modo sicuro AWS senza che i team di sicurezza o di sviluppo delle applicazioni abbiano esperienza in AI/ML.

L'intelligenza artificiale è una tecnologia avanzata che consente a macchine e sistemi di acquisire intelligenza e capacità di previsione. I sistemi di intelligenza artificiale imparano dall'esperienza passata attraverso i dati che utilizzano o sui quali vengono addestrati. L'apprendimento automatico è uno degli aspetti più importanti dell'IA. L'apprendimento automatico è la capacità dei computer di apprendere dai dati senza essere programmati esplicitamente. Nella programmazione tradizionale, il programmatore scrive regole che definiscono come il programma dovrebbe funzionare su un computer o una macchina. In ML, il modello impara le regole dai dati. I modelli ML possono scoprire schemi nascosti nei dati o fare previsioni accurate su nuovi dati che non sono stati utilizzati durante l'addestramento. Servizi AWS Uso multiplo AI/ML per imparare da enormi set di dati e fare inferenze sulla sicurezza.

- Amazon Macie è un servizio di sicurezza dei dati che utilizza il machine learning e il pattern matching per scoprire e proteggere i tuoi dati sensibili. Macie rileva automaticamente un ampio e crescente elenco di tipi di dati sensibili, tra cui informazioni di identificazione personale (PII) come nomi, indirizzi e informazioni finanziarie come numeri di carte di credito. Inoltre, ti offre una visibilità costante sui dati archiviati in Amazon Simple Storage Service (Amazon S3). Macie utilizza modelli di elaborazione del linguaggio naturale (NLP) e ML addestrati su diversi tipi di set di dati per comprendere i dati esistenti e assegnare valori aziendali per dare priorità ai dati aziendali critici. Macie genera quindi risultati di dati sensibili.
- Amazon GuardDuty è un servizio di rilevamento delle minacce che utilizza il machine learning, il rilevamento delle anomalie e l'intelligence integrata sulle minacce per monitorare continuamente attività dannose e comportamenti non autorizzati e proteggere i carichi di lavoro, gli utenti Account AWS, i database e lo storage, le istanze, le istanze, i carichi di lavoro serverless e container. GuardDuty incorpora tecniche di machine learning estremamente efficaci nel distinguere le

attività potenzialmente dannose degli utenti da quelle interne a comportamenti operativi anomali ma benigni. Account AWS Questa funzionalità modella continuamente le chiamate alle API all'interno di un account e incorpora previsioni probabilistiche per isolare e avvisare in modo più accurato i comportamenti altamente sospetti degli utenti. Questo approccio aiuta a identificare le attività dannose associate a tattiche di minaccia note, tra cui il rilevamento, l'accesso iniziale, la persistenza, l'escalation dei privilegi, l'evasione della difesa, l'accesso alle credenziali, l'impatto e l'esfiltrazione dei dati. Per ulteriori informazioni su come GuardDuty utilizza l'apprendimento automatico, consulta la sessione di approfondimento di AWS RE:InForce 2023 Sviluppare nuove scoperte utilizzando l'apprendimento automatico in Amazon GuardDuty (0). TDR31

Sicurezza dimostrabile

AWS sviluppa strumenti di ragionamento automatizzato che utilizzano la logica matematica per rispondere a domande critiche sull'infrastruttura e per rilevare configurazioni errate che potrebbero potenzialmente esporre i dati. Questa funzionalità è chiamata sicurezza dimostrabile perché offre una maggiore garanzia nella sicurezza del cloud e nel cloud. La sicurezza dimostrabile utilizza il ragionamento automatico, che è una disciplina specifica dell'intelligenza artificiale che applica la deduzione logica ai sistemi informatici. Ad esempio, gli strumenti di ragionamento automatico possono analizzare le policy e le configurazioni dell'architettura di rete e dimostrare l'assenza di configurazioni involontarie che potrebbero potenzialmente esporre dati vulnerabili. Questo approccio offre il massimo livello di garanzia possibile per le caratteristiche di sicurezza critiche del cloud. Per ulteriori informazioni, consulta Provable Security Resources sul AWS sito Web. Le seguenti Servizi AWS funzionalità utilizzano attualmente il ragionamento automatico per aiutarti a ottenere una sicurezza dimostrabile per le tue applicazioni:

- Amazon Verified Permissions è un servizio scalabile di gestione delle autorizzazioni e di autorizzazione granulare per le applicazioni che crei. Verified Permissions utilizza Cedar, un linguaggio open source per il controllo degli accessi creato utilizzando ragionamenti automatici e test differenziali. Cedar è un linguaggio per definire le autorizzazioni come politiche che descrivono chi deve avere accesso a quali risorse. È anche una specifica per la valutazione di tali politiche. Utilizzate le politiche Cedar per controllare ciò che ogni utente della vostra applicazione è autorizzato a fare e a quali risorse può accedere. Le politiche Cedar sono dichiarazioni di autorizzazione o divieto che determinano se un utente può agire su una risorsa. Le politiche sono associate alle risorse ed è possibile allegare più politiche a una risorsa. Le politiche di divieto hanno la precedenza sulle politiche di autorizzazione. Quando un utente dell'applicazione tenta di eseguire un'azione su una risorsa, l'applicazione invia una richiesta di autorizzazione al motore di

policy Cedar. Cedar valuta le politiche applicabili e restituisce una `ALLOW` decisione or. `DENY` Cedar supporta le regole di autorizzazione per qualsiasi tipo di principale e risorsa, consente il controllo degli accessi basato sui ruoli e sugli attributi e supporta l'analisi tramite strumenti di ragionamento automatizzati che possono aiutare a ottimizzare le politiche e a convalidare il modello di sicurezza.

- AWS Identity and Access Management Access Analyzerti aiuta a semplificare la gestione delle autorizzazioni. È possibile utilizzare questa funzionalità per impostare autorizzazioni dettagliate, verificare le autorizzazioni previste e perfezionare le autorizzazioni rimuovendo l'accesso non utilizzato. IAM Access Analyzer genera una policy dettagliata basata sull'attività di accesso acquisita nei log. Fornisce inoltre oltre 100 controlli delle politiche per aiutarti a creare e convalidare le tue politiche. IAM Access Analyzer utilizza una sicurezza comprovabile per analizzare i percorsi di accesso e fornire risultati completi per l'accesso pubblico e interaccount alle risorse. Questo strumento è basato su Zelkova, che traduce le politiche IAM in istruzioni logiche equivalenti ed esegue una suite di risolutori logici generici e specializzati (teorie dei moduli di soddisfacibilità) per risolvere il problema. Sistema di analisi degli accessi AWS IAM applica Zelkova ripetutamente a una policy con query sempre più specifiche per caratterizzare classi di comportamenti consentite dalla policy, in base al contenuto della policy stessa. L'analizzatore non esamina i log di accesso per determinare se un'entità esterna ha avuto accesso a una risorsa all'interno della zona di fiducia dell'utente. Genera un risultato quando una politica basata sulle risorse consente l'accesso a una risorsa, anche se l'entità esterna non ha avuto accesso alla risorsa. Per saperne di più sulle teorie dei moduli di soddisfacibilità, vedi Satisfiability Modulo Theories in Handbook of Satisfiability. *
- Amazon S3 Block Public Access è una funzionalità di Amazon S3 che consente di bloccare possibili configurazioni errate che potrebbero portare all'accesso pubblico ai bucket e agli oggetti. Puoi abilitare Amazon S3 Block Public Access per punti di accesso, bucket, account e AWS organizzazione (il che influisce sia sui bucket esistenti che su quelli nuovi nell'account). L'accesso pubblico a bucket e oggetti viene concesso tramite liste di controllo degli accessi (ACLs), policy di bucket o entrambe. La determinazione se una determinata politica o ACL è considerata pubblica viene effettuata utilizzando il sistema di ragionamento automatico Zelkova. Amazon S3 utilizza Zelkova per verificare la policy di ogni bucket e ti avvisa se un utente non autorizzato è in grado di leggere o scrivere nel tuo bucket. Se un bucket è contrassegnato come pubblico, alcune richieste pubbliche possono accedere al bucket. Se un bucket è contrassegnato come non pubblico, tutte le richieste pubbliche vengono rifiutate. Zelkova è in grado di effettuare tali determinazioni perché ha una rappresentazione matematica precisa delle politiche IAM. Crea una formula per ogni politica e dimostra un teorema su quella formula.
- Amazon VPC Network Access Analyzer è una funzionalità di Amazon VPC che ti aiuta a comprendere i potenziali percorsi di rete verso le tue risorse e a identificare potenziali accessi non

intenzionali alla rete. Network Access Analyzer ti aiuta a verificare la segmentazione della rete, identificare l'accessibilità a Internet e verificare percorsi di rete e accessi alla rete affidabili. Questa funzionalità utilizza algoritmi di ragionamento automatico per analizzare i percorsi di rete che un pacchetto può percorrere tra le risorse di una rete. AWS Quindi produce risultati per i percorsi che corrispondono agli ambiti di accesso alla rete, che definiscono i modelli di traffico in uscita e in entrata. Strumento di analisi degli accessi alla rete esegue un'analisi statica di una configurazione di rete, il che significa che nessun pacchetto viene trasmesso nella rete come parte di questa analisi.

- Amazon VPC Reachability Analyzer è una funzionalità di Amazon VPC che consente di eseguire il debug, comprendere e visualizzare la connettività nella rete. AWS Reachability Analyzer è uno strumento di analisi della configurazione che consente di eseguire test di connettività tra una risorsa di origine e una risorsa di destinazione nei cloud privati virtuali (). VPCs Quando la destinazione è raggiungibile, Reachability Analyzer hop-by-hop produce dettagli sul percorso di rete virtuale tra l'origine e la destinazione. Quando la destinazione non è raggiungibile, Reachability Analyzer identifica il componente di blocco. Reachability Analyzer utilizza il ragionamento automatico per identificare percorsi possibili costruendo un modello della configurazione di rete tra un'origine e una destinazione. Quindi verifica la raggiungibilità in base alla configurazione. Non invia pacchetti né analizza il piano dati.

* Biere, A. M. Heule, H. van Maaren e T. Walsh. 2009. Manuale di soddisfacibilità. IOS Press, NLD.

Costruire la propria architettura di sicurezza: un approccio graduale

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

L'architettura di sicurezza multi-account consigliata dalla AWS SRA è un'architettura di base che consente di inserire la sicurezza nelle prime fasi del processo di progettazione. Il percorso verso il cloud di ogni organizzazione è unico. Per far evolvere con successo la vostra architettura di sicurezza cloud, dovete immaginare lo stato di destinazione desiderato, comprendere la vostra attuale preparazione al cloud e adottare un approccio agile per colmare eventuali lacune. L' AWS SRA fornisce uno stato obiettivo di riferimento per l'architettura di sicurezza. La trasformazione incrementale consente di dimostrare rapidamente il valore aggiunto riducendo al minimo la necessità di fare previsioni di ampia portata.

Il AWS Cloud Adoption Framework (AWS CAF) consiglia quattro fasi iterative e incrementali di trasformazione del cloud: immagina, allinea, lancia e scala. Quando entri nella fase di lancio e ti concentri sulla realizzazione di iniziative pilota in produzione, dovresti concentrarti sulla creazione di una solida architettura di sicurezza come base per la fase di scalabilità, in modo da avere la capacità tecnica di migrare e gestire i carichi di lavoro più critici per l'azienda con sicurezza. Questo approccio graduale è applicabile se sei una startup, una piccola o media azienda che desidera espandere la propria attività o un'azienda che sta acquisendo nuove unità aziendali o sta effettuando fusioni e acquisizioni. L' AWS SRA ti aiuta a raggiungere quell'architettura di base di sicurezza in modo da poter applicare i controlli di sicurezza in modo uniforme in tutta la tua organizzazione in espansione. AWS Organizations L'architettura di base è composta da più servizi. Account AWS La pianificazione e l'implementazione devono essere un processo in più fasi in modo da poter eseguire iterazioni su traguardi più piccoli per raggiungere l'obiettivo principale di configurare l'architettura di sicurezza di base. Questa sezione descrive le fasi tipiche del tuo percorso verso il cloud sulla base di un approccio strutturato. Queste fasi sono in linea con i principi di progettazione della sicurezza del AWS Well-Architected Framework.

Fase 1: creazione dell'unità organizzativa e della struttura degli account

Un prerequisito per una solida base di sicurezza è un' AWS organizzazione e una struttura degli account ben progettate. Come spiegato in precedenza nella sezione sugli elementi costitutivi SRA di questa guida, averne più di uno Account AWS aiuta a isolare diverse funzioni aziendali e di sicurezza in base alla progettazione. All'inizio potrebbe sembrare un lavoro inutile, ma è un investimento per aiutarvi a scalare in modo rapido e sicuro. Questa sezione spiega anche come gestire più Account AWS account e come AWS Organizations utilizzare le funzionalità di accesso affidabile e di amministratore delegato per la gestione Servizi AWS centralizzata di più account.

Puoi usare AWS Control Towerquanto descritto in precedenza in questa guida per orchestrare la tua landing zone. Se al momento ne utilizzi uno Account AWS, consulta la Account AWS guida sulla transizione a più account per migrare a più account il prima possibile. Ad esempio, se la tua startup sta attualmente ideando e prototipando il tuo prodotto in un unico prodotto Account AWS, dovresti prendere in considerazione l'adozione di una strategia multi-account prima di lanciare il prodotto sul mercato. Allo stesso modo, le organizzazioni di piccole, medie e imprese dovrebbero iniziare a sviluppare la propria strategia multi-account non appena pianificano i carichi di lavoro di produzione iniziali. Inizia con la tua fondazione Account AWS, quindi aggiungi OUs gli account e gli account relativi al carico di lavoro OUs .

Per Account AWS consigli sulla struttura delle unità organizzative oltre a quelli forniti nell' AWS SRA, consulta il post sul blog Strategia multiaccount per le piccole e medie imprese. Mentre stai finalizzando la struttura dell'unità organizzativa e degli account, prendi in considerazione i controlli di sicurezza di alto livello a livello di organizzazione che vorresti applicare utilizzando le politiche di controllo dei servizi (SCPs), le politiche di controllo delle risorse () e le politiche dichiarative. RCPs

> **Considerazione di natura progettuale**
>
> Non replicate la struttura di rendicontazione della vostra azienda quando progettate l'unità organizzativa e la struttura degli account. È OUs necessario basarsi sulle funzioni del carico di lavoro e su una serie comune di controlli di sicurezza applicabili ai carichi di lavoro.
> Non cercare di progettare la struttura completa del conto fin dall'inizio. Concentrati sulle funzionalità di base OUs, quindi aggiungi il carico di lavoro in base OUs alle tue esigenze. Puoi spostare gli account da un account OUs all'altro per sperimentare approcci alternativi durante le prime fasi della progettazione. Tuttavia, ciò potrebbe comportare un sovraccarico

relativo alla gestione delle autorizzazioni logiche, a seconda SCPs delle policy dichiarative e delle condizioni IAM basate sull'unità organizzativa e sui percorsi degli account. RCPs

Esempio di implementazione

La libreria di codici AWS SRA fornisce un'implementazione di esempio di Account Alternate Contacts. Questa soluzione imposta i contatti alternativi di fatturazione, operazioni e sicurezza per tutti gli account all'interno di un'organizzazione.

Fase 2: Implementazione di una solida base di identità

Non appena ne avrai creati più di uno Account AWS, dovresti consentire ai tuoi team di accedere alle AWS risorse all'interno di tali account. Esistono due categorie generali di gestione delle identità: gestione delle identità e degli accessi della forza lavoro e gestione delle identità e degli accessi dei clienti (CIAM). Workforce IAM è destinato alle organizzazioni in cui dipendenti e carichi di lavoro automatizzati devono accedere AWS per svolgere il proprio lavoro. CIAM viene utilizzato quando un'organizzazione ha bisogno di un modo per autenticare gli utenti per fornire l'accesso alle applicazioni dell'organizzazione. È innanzitutto necessaria una strategia IAM per la forza lavoro, in modo che i team possano creare e migrare le applicazioni. Dovresti sempre utilizzare i ruoli IAM anziché gli utenti IAM per fornire l'accesso a utenti umani o automatici. Segui le indicazioni AWS SRA su come utilizzare all' AWS IAM Identity Center interno degli account Org Management e Shared Services per gestire centralmente l'accesso Single Sign-On (SSO) al tuo. Account AWS La guida fornisce anche considerazioni di progettazione per l'utilizzo della federazione IAM quando non è possibile utilizzare IAM Identity Center.

Quando lavori con i ruoli IAM per fornire agli utenti l'accesso alle AWS risorse, dovresti utilizzare IAM Access Analyzer e IAM access advisor, come indicato nelle sezioni Security Tooling e Org Management di questa guida. Questi servizi ti aiutano a ottenere il privilegio minimo, un importante controllo preventivo che ti aiuta a creare un buon livello di sicurezza.

Considerazione di natura progettuale

Per ottenere il privilegio minimo, progettate processi che consentano di rivedere e comprendere regolarmente le relazioni tra le vostre identità e le autorizzazioni necessarie per funzionare correttamente. Man mano che impari, perfeziona tali autorizzazioni e riducile

gradualmente al minimo possibile. Per quanto riguarda la scalabilità, questa dovrebbe essere una responsabilità condivisa tra i team di sicurezza centrale e i team addetti alle applicazioni. Utilizzate funzionalità come policy basate sulle risorse, limiti di autorizzazione, controlli di accesso basati sugli attributi e policy di sessione per aiutare i proprietari delle applicazioni a definire un controllo granulare degli accessi.

Esempi di implementazione

La libreria di codici AWS SRA fornisce due implementazioni di esempio che si applicano a questa fase:

- IAM Password Policy imposta la politica relativa alle password degli account per consentire agli utenti di allinearsi agli standard di conformità comuni.
- Access Analyzer configura un analizzatore a livello di organizzazione all'interno di un account amministratore delegato e un analizzatore a livello di account all'interno di ciascun account.

Fase 3: mantenimento della tracciabilità

Quando gli utenti avranno accesso AWS e inizieranno a creare, vorrai sapere chi sta facendo cosa, quando e da dove. Avrai anche bisogno di visibilità su potenziali configurazioni errate di sicurezza, minacce o comportamenti imprevisti. Una migliore comprensione delle minacce alla sicurezza consente di dare priorità ai controlli di sicurezza appropriati. Per monitorare AWS l'attività, segui i consigli AWS SRA per configurare un percorso organizzativo utilizzando AWS CloudTraile centralizzando i log all'interno dell'account Log Archive. Per il monitoraggio degli eventi di sicurezza AWS Security Hub CSPM, usa Amazon GuardDuty e Amazon Security Lake come indicato nella sezione Account Security Tooling. AWS Config

Considerazione di natura progettuale

Quando inizi a utilizzarne di nuovi Servizi AWS, assicurati di abilitare i log specifici del servizio e di archiviarli come parte del tuo archivio centrale dei log.

Esempi di implementazione

La libreria di codici AWS SRA fornisce le seguenti implementazioni di esempio che si applicano a questa fase:

- L'organizzazione CloudTrail crea un percorso organizzativo e imposta le impostazioni predefinite per configurare gli eventi relativi ai dati (ad esempio, in Amazon S3 AWS Lambda e) per ridurre la duplicazione CloudTrail di ciò da cui è configurato. AWS Control Tower Questa soluzione offre opzioni per la configurazione degli eventi di gestione.
- AWS Config L'account di gestione Control Tower consente AWS Config all'account di gestione di monitorare la conformità delle risorse.
- Conformance Pack Organization Rules distribuisce un pacchetto di conformità agli account e alle regioni specificate all'interno di un'organizzazione.
- AWS Config Aggregator implementa un aggregatore delegando l'amministrazione a un account membro diverso dall'account Audit.
- Security Hub CSPM Organization configura Security Hub CSPM all'interno di un account amministratore delegato per gli account e le regioni gestite all'interno dell'organizzazione.
- GuardDuty L'organizzazione si configura GuardDuty all'interno di un account amministratore delegato per gli account all'interno di un'organizzazione.

Fase 4: applicare la sicurezza a tutti i livelli

A questo punto, dovresti avere:

- I controlli di sicurezza appropriati per il tuo Account AWS.
- Una struttura di account e unità organizzative ben definiti con controlli preventivi definiti tramite SCPs politiche dichiarative e ruoli e policy IAM con privilegi minimi. RCPs
- La capacità di registrare AWS le attività utilizzando AWS CloudTrail; di rilevare eventi di sicurezza utilizzando AWS Security Hub CSPM Amazon GuardDuty e AWS Config; e di eseguire analisi avanzate su un data lake creato appositamente per la sicurezza utilizzando Amazon Security Lake.

In questa fase, pianifica di applicare la sicurezza ad altri livelli della tua AWS organizzazione, come descritto nella sezione Applica i servizi di sicurezza in tutta l'organizzazione. AWS Puoi creare controlli di sicurezza per il tuo livello di rete utilizzando servizi come AWS WAF,, AWS Shield, AWS

Firewall ManagerAWS Network Firewall, AWS Certificate Manager (ACM), Amazon CloudFront, Amazon Route 53 e Amazon VPC, come indicato nella sezione Account di rete. Man mano che procedi verso il basso dello stack tecnologico, applica controlli di sicurezza specifici per il carico di lavoro o lo stack di applicazioni. Utilizza gli endpoint VPC, Amazon Inspector AWS Systems Manager e Gestione dei segreti AWS Amazon Cognito come indicato nella sezione Account dell'applicazione.

Considerazione di natura progettuale

Mentre progetti i controlli di sicurezza DiD (Defense In Depth), prendi in considerazione i fattori di scalabilità. Il tuo team di sicurezza centrale non avrà la larghezza di banda o la piena comprensione del comportamento di ogni applicazione nel tuo ambiente. Consentite ai vostri team applicativi di assumersi la responsabilità e la responsabilità di identificare e progettare i controlli di sicurezza giusti per le loro applicazioni. Il team di sicurezza centrale dovrebbe concentrarsi sulla fornitura degli strumenti e della consulenza giusti per supportare i team addetti alle applicazioni. Per comprendere i meccanismi di scalabilità AWS utilizzati per adottare un approccio alla sicurezza più orientato verso sinistra, consulta il post sul blog How AWS built the Security Guardians program, a mechanism to distribute security ownership.

Esempi di implementazione

La libreria di codici AWS SRA fornisce le seguenti implementazioni di esempio che si applicano a questa fase:

- EC2 Default EBS Encryption configura la crittografia Amazon EBS predefinita in Amazon EC2 per utilizzare quella predefinita all'interno di quella fornita. AWS KMS key Regioni AWS
- S3 Block Account Public Access configura le impostazioni Block Public Access (BPA) a livello di account in Amazon S3 per gli account all'interno dell'organizzazione.
- Firewall Manager dimostra come configurare una politica e delle AWS WAF politiche dei gruppi di sicurezza per gli account all'interno di un'organizzazione.
- Inspector Organization configura Amazon Inspector all'interno di un account amministratore delegato per gli account e le regioni governate all'interno dell'organizzazione.

Fase 5: protezione dei dati in transito e a riposo

I dati aziendali e dei clienti sono risorse preziose che devi proteggere. AWS fornisce vari servizi e funzionalità di sicurezza per proteggere i dati in movimento e a riposo. Usa Amazon CloudFront con AWS Certificate Manager, come indicato nella sezione Account di rete, per proteggere i dati in movimento raccolti su Internet. Per i dati in movimento all'interno delle reti interne, utilizzate un Application Load Balancer con AWS Autorità di certificazione privata, come spiegato nella sezione Account dell'applicazione. AWS KMS e ti AWS CloudHSM aiutano a fornire una gestione delle chiavi crittografiche per proteggere i dati inattivi.

Fase 6: preparazione per gli eventi di sicurezza

Durante la gestione dell'ambiente IT, si verificheranno eventi di sicurezza, ossia cambiamenti nel funzionamento quotidiano dell'ambiente IT che indicano una possibile violazione delle politiche di sicurezza o un fallimento del controllo di sicurezza. Una tracciabilità adeguata è fondamentale per essere consapevoli di un evento di sicurezza il più rapidamente possibile. È altrettanto importante essere preparati a valutare e rispondere a tali eventi di sicurezza in modo da poter intraprendere le azioni appropriate prima che l'evento di sicurezza si aggravi. La preparazione consente di valutare rapidamente un evento di sicurezza per comprenderne il potenziale impatto.

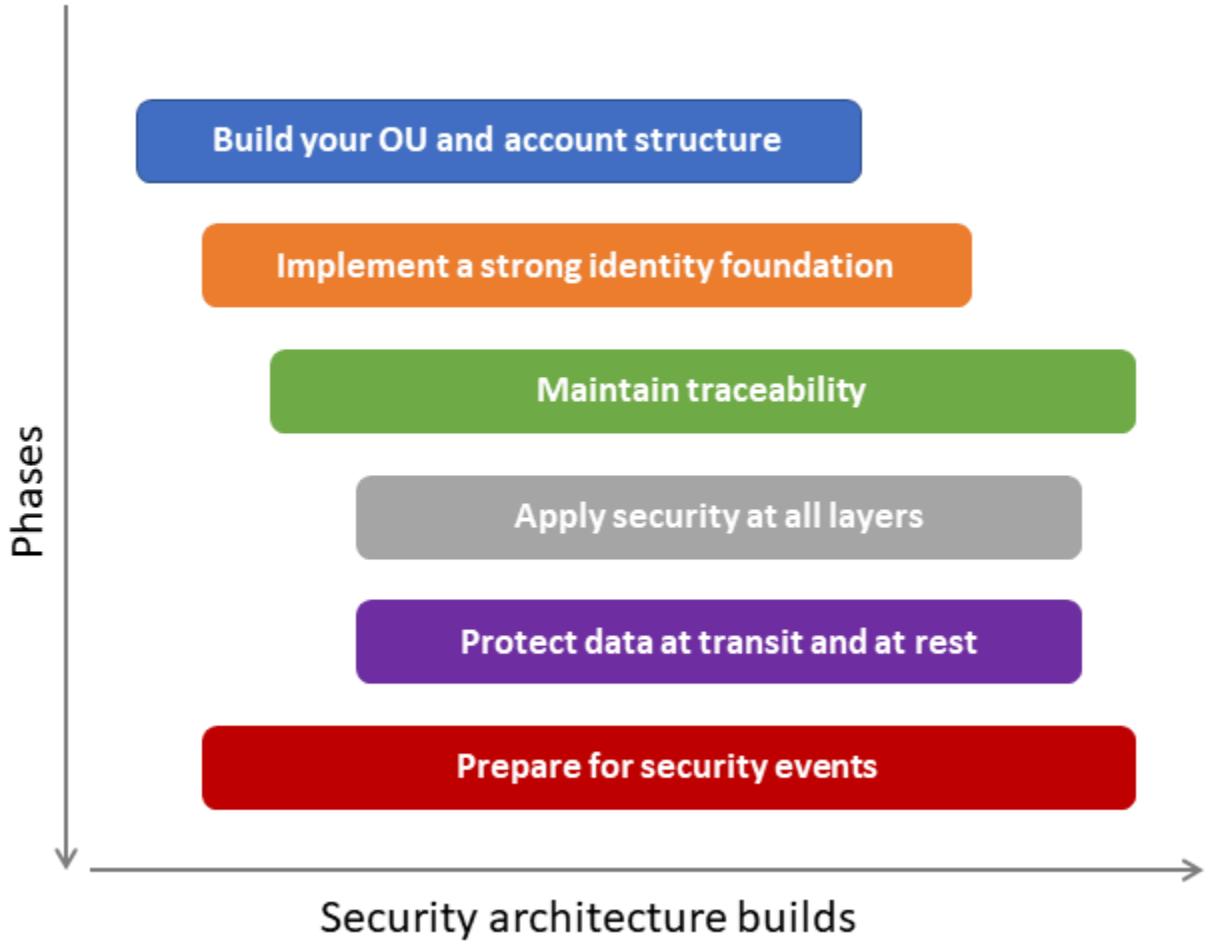
L' AWS SRA, attraverso la progettazione dell'account Security Tooling e l'implementazione di servizi di sicurezza comuni a tutti Account AWS, offre la possibilità di rilevare gli eventi di sicurezza all'interno dell'organizzazione. AWS Amazon Detective all'interno dell'account Security Tooling ti aiuta a valutare un evento di sicurezza e a identificarne la causa principale. Durante un'indagine di sicurezza, devi essere in grado di esaminare i log pertinenti per registrarli e comprendere l'ambito e la tempistica completi dell'incidente. I registri sono necessari anche per la generazione di avvisi quando si verificano azioni di interesse specifiche. L' AWS SRA consiglia un account Log Archive centrale per l'archiviazione immutabile di tutti i registri operativi e di sicurezza. Puoi interrogare i log utilizzando CloudWatch Logs Insights per i dati archiviati in gruppi di CloudWatch log e Amazon Athena e Amazon Service per i dati archiviati in Amazon S3. OpenSearch Usa Amazon Security Lake per centralizzare automaticamente i dati di sicurezza provenienti dall' AWS ambiente, dai provider di software as a service (SaaS), dagli ambienti locali e da altri provider cloud. Configura gli abbonati nell'account Security Tooling o in qualsiasi account dedicato, come indicato dall' AWS SRA, per interrogare i log e analizzarli.

AWS Security Incident Responseti aiuta ad automatizzare la risposta, l'indagine e la correzione degli incidenti di sicurezza. Fornisce playbook e flussi di lavoro predefiniti per aiutarti a rispondere agli

eventi di sicurezza in modo rapido e coerente. Quando la funzionalità di risposta proattiva è abilitata, Security Incident Response si integra con Security Hub CSPM e GuardDuty attiva automaticamente i flussi di lavoro di risposta quando vengono rilevati problemi di sicurezza. Il servizio consente di standardizzare e automatizzare i processi di risposta agli incidenti in tutta l'organizzazione. AWS Se hai bisogno di ulteriore assistenza, puoi aprire una richiesta supportata dal servizio e contattare il AWS Customer Incident Response Team (CIRT).

Considerazioni di natura progettuale

- Dovresti iniziare a prepararti a rilevare e rispondere agli eventi di sicurezza sin dall'inizio del tuo percorso verso il cloud. Per utilizzare al meglio le risorse limitate, assegnate i dati e la criticità aziendale alle vostre AWS risorse in modo che, quando rilevate un evento di sicurezza, possiate dare priorità alla valutazione e alla risposta in base alla criticità delle risorse coinvolte.
- Le fasi per la creazione dell'architettura di sicurezza cloud, come illustrato in questa sezione, sono di natura sequenziale. Tuttavia, non è necessario attendere il completamento completo di una fase prima di iniziare la fase successiva. Ti consigliamo di adottare un approccio iterativo, in cui inizi a lavorare su più fasi in parallelo e ad evolvere ogni fase man mano che evolvi la tua posizione di sicurezza sul cloud. Man mano che attraverserai le diverse fasi, il tuo design si evolverà. Valuta la possibilità di personalizzare la sequenza suggerita mostrata nel diagramma seguente in base alle tue esigenze particolari.



Esempio di implementazione

La libreria di codici AWS SRA fornisce un'implementazione di esempio di un'organizzazione investigativa, che abilita automaticamente Amazon Detective delegando l'amministrazione a un account (ad esempio, Audit o Security Tooling) e configura Detective per account esistenti e futuri. AWS Organizations

AWS Elenco di controllo delle migliori pratiche SRA

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

Questa sezione riassume le migliori pratiche AWS SRA descritte in questa guida in una lista di controllo da seguire quando si crea la propria versione dell'architettura di sicurezza. AWS Utilizzate questo elenco come punto di riferimento e non come sostituto della revisione della guida. La lista di controllo è raggruppata per. Servizio AWSSe desideri convalidare a livello di codice AWS l'ambiente esistente rispetto alla checklist delle migliori pratiche AWS SRA, puoi utilizzare SRA Verify.

SRA Verify è uno strumento di valutazione della sicurezza che consente di valutare l'allineamento dell'organizzazione all'SRA in più regioni. AWS Account AWS Si basa direttamente sulle raccomandazioni AWS SRA fornendo controlli automatici che convalidano l'implementazione rispetto alle linee guida SRA. AWS Lo strumento consente di verificare che i servizi di sicurezza siano configurati correttamente in base all'architettura di riferimento. Fornisce risultati dettagliati e misure correttive attuabili per garantire che l' AWS ambiente segua le migliori pratiche di sicurezza. SRA Verify è progettato per essere eseguito AWS CodeBuild nell'account di controllo dell'organizzazione (Security Tooling). Puoi anche eseguirlo localmente o estenderlo utilizzando la libreria SRA Verify.

> **Note**
>
> SRA Verify contiene controlli per diversi servizi, ma potrebbe non contenere un controllo per ogni aspetto dell' AWS SRA. Per ulteriori informazioni, consulta le guide nella libreria AWS SRA.

AWS Organizations

- AWS Organizations è abilitato con tutte le funzionalità.
- Le policy di controllo dei servizi (SCPs) vengono utilizzate per definire le linee guida per il controllo degli accessi per i responsabili IAM.
- Le politiche di controllo delle risorse (RCPs) vengono utilizzate per definire le linee guida per il controllo degli accessi alle AWS risorse.

- Le politiche dichiarative vengono utilizzate per dichiarare e applicare centralmente la configurazione desiderata per un determinato periodo su larga scala Servizio AWS all'interno dell'organizzazione.
- OUs Vengono creati tre account di base (Sicurezza, Infrastruttura e Carico di lavoro) per raggruppare gli account dei membri che forniscono servizi di base.
- L'account Security Tooling viene creato nell'unità organizzativa di sicurezza. Questo account fornisce la gestione centralizzata dei servizi di AWS sicurezza e di altri strumenti di sicurezza di terze parti.
- L'account Log Archive viene creato nell'unità organizzativa di sicurezza. Questo account fornisce un archivio centrale di registri Servizi AWS e registri delle applicazioni strettamente controllato.
- L'account di rete viene creato nell'unità organizzativa dell'infrastruttura. Questo account gestisce il gateway tra l'applicazione e Internet in generale. Isola i servizi di rete, la configurazione e il funzionamento dai carichi di lavoro delle singole applicazioni, dalla sicurezza e da altre infrastrutture.
- L'account Shared Service viene creato nell'unità organizzativa dell'infrastruttura. Questo account supporta i servizi utilizzati da più applicazioni e team per fornire i propri risultati.
- L'account dell'applicazione viene creato nell'unità organizzativa Workloads. Questo account ospita l'infrastruttura e i servizi principali per l'esecuzione e la manutenzione di un'applicazione aziendale. Questa guida fornisce una rappresentazione, ma nel mondo reale ci saranno account multipli OUs e membri separati per applicazioni, ambienti di sviluppo e altre considerazioni sulla sicurezza.
- Sono configurate informazioni di contatto alternative per la fatturazione, le operazioni e la sicurezza per tutti gli account dei membri.

AWS CloudTrail

- È configurato un percorso organizzativo che consente la distribuzione degli eventi di CloudTrail gestione nell'account di gestione e in tutti gli account dei membri di un' AWS organizzazione.
- L'itinerario organizzativo è configurato come percorso multiregionale.
- L'organigramma è configurato per acquisire eventi da risorse globali.
- Se necessario, vengono configurati percorsi aggiuntivi per l'acquisizione di eventi relativi ai dati specifici per monitorare le attività relative alle AWS risorse sensibili.
- L'account Security Tooling è impostato come amministratore delegato dell'organigramma.

- L'organigramma è configurato per essere abilitato automaticamente per tutti i nuovi account membro.
- L'organigramma è configurato per pubblicare i log in un bucket S3 centralizzato ospitato nell'account Log Archive.
- L'organigramma ha abilitato la convalida dei file di registro per verificare l'integrità dei file di registro.
- L'organigramma è integrato con CloudWatch Logs per la conservazione dei log.
- L'organigramma è crittografato utilizzando una chiave gestita dal cliente.
- Il bucket S3 centrale utilizzato per l'archivio dei log nell'account Log Archive è crittografato con una chiave gestita dal cliente.
- Il bucket S3 centrale utilizzato per l'archivio dei log nell'account Log Archive è configurato con S3 Object Lock per l'immutabilità.
- Il controllo delle versioni è abilitato per il bucket S3 centrale utilizzato per l'archivio dei log nell'account Log Archive.
- Il bucket S3 centrale utilizzato per l'archivio dei log nell'account Log Archive ha una politica delle risorse definita che limita il caricamento degli oggetti solo tramite il percorso organizzativo attraverso la risorsa Amazon Resource Name (ARN).

AWS Security Hub CSPM

- Security Hub CSPM è abilitato per tutti gli account dei membri e per l'account di gestione.
- AWS Config è abilitato per tutti gli account dei membri come prerequisito per Security Hub CSPM.
- L'account Security Tooling è impostato come amministratore delegato di Security Hub CSPM.
- Amazon GuardDuty e Amazon Detective hanno lo stesso account amministratore delegato del Security Hub CSPM per una perfetta integrazione dei servizi.
- La configurazione centrale viene utilizzata per configurare e gestire Security Hub CSPM su più Account AWS e. Regioni AWS
- Tutte le unità organizzative e gli account dei membri sono designati come gestiti centralmente dall'amministratore delegato di Security Hub CSPM.
- Security Hub CSPM è abilitato automaticamente per tutti gli account dei nuovi membri.
- Security Hub CSPM è abilitato automaticamente per la configurazione di nuovi standard.
- I risultati CSPM di Security Hub di tutte le regioni vengono aggregati in un'unica area geografica.

- I risultati CSPM di Security Hub di tutti gli account dei membri vengono aggregati all'interno dell'account Security Tooling.
- Lo standard AWS Foundational Best Practices (FSBP) in Security Hub CSPM è abilitato per tutti gli account dei membri.
- Lo standard CIS AWS Foundation Benchmark in Security Hub CSPM è abilitato per tutti gli account dei membri.
- Se applicabile, sono abilitati altri standard CSPM di Security Hub.
- Una regola di automazione CSPM di Security Hub viene utilizzata per arricchire i risultati con il contesto delle risorse.
- La funzionalità di risposta e correzione automatizzata Security Hub CSPM viene utilizzata per creare EventBridge regole personalizzate per intraprendere azioni automatiche in base a risultati specifici.

AWS Config

- Il AWS Config registratore è abilitato per tutti gli account dei membri e per l'account di gestione.
- Il AWS Config registratore è abilitato per tutte le regioni.
- Il bucket S3 del canale di AWS Config distribuzione è centralizzato nell'account Log Archive.
- L'account amministratore AWS Config delegato è impostato sull'account Security Tooling.
- AWS Config ha un aggregatore di organizzazioni configurato. L'aggregatore include tutte le regioni.
- AWS Config i pacchetti di conformità vengono distribuiti in modo uniforme su tutti gli account dei membri a partire dall'account amministratore delegato.
- AWS Config i risultati delle regole vengono inviati automaticamente a Security Hub CSPM.

Amazon GuardDuty

- GuardDuty il rilevatore è abilitato per tutti gli account dei membri e per l'account di gestione.
- GuardDuty il rilevatore è abilitato per tutte le regioni.
- GuardDuty il rilevatore è abilitato automaticamente per tutti gli account dei nuovi membri.
- GuardDuty l'amministrazione delegata è impostata sull'account Security Tooling.
- GuardDuty sono abilitate fonti di dati fondamentali come eventi di CloudTrail gestione, log di flusso VPC e log di query DNS di Route 53 Resolver.

- GuardDuty La protezione S3 è abilitata.
- GuardDuty La protezione da malware per i volumi EBS è abilitata.
- GuardDuty La protezione da malware per S3 è abilitata.
- GuardDuty La protezione RDS è abilitata.
- GuardDuty La protezione Lambda è abilitata.
- GuardDuty La protezione EKS è abilitata.
- GuardDuty EKS Runtime Monitoring è abilitato.
- GuardDuty Il rilevamento esteso delle minacce è abilitato.
- GuardDuty i risultati vengono esportati in un bucket S3 centrale nell'account Log Archive per essere conservati.

IAM

- Gli utenti IAM non vengono utilizzati.
- Viene applicata la gestione centralizzata dell'accesso root per gli account dei membri.
- L'attività centralizzata dell'utente root privilegiato per l'account di gestione viene applicata dall'amministratore delegato.
- La gestione centralizzata degli accessi root è delegata all'account Security Tooling.
- Tutte le credenziali root dell'account membro vengono rimosse.
- Tutte le politiche relative alle Account AWS password dei membri e dei gestori sono impostate in base allo standard di sicurezza dell'organizzazione.
- IAM access advisor viene utilizzato per esaminare le ultime informazioni utilizzate per gruppi, utenti, ruoli e politiche IAM.
- I limiti di autorizzazione vengono utilizzati per limitare il numero massimo di autorizzazioni possibili per i ruoli IAM.

Sistema di analisi degli accessi IAM

- IAM Access Analyzer è abilitato per tutti gli account dei membri e per l'account di gestione.
- L'amministratore delegato di IAM Access Analyzer è impostato sull'account Security Tooling.
- L'analizzatore di accesso esterno IAM Access Analyzer è configurato con la zona di fiducia dell'organizzazione in ogni regione.

- L'analizzatore di accesso esterno IAM Access Analyzer è configurato con la zona di fiducia dell'account in ogni regione.
- L'analizzatore di accesso interno IAM Access Analyzer è configurato con la zona di fiducia dell'organizzazione in ogni regione.
- L'analizzatore di accesso interno IAM Access Analyzer è configurato con la zona di fiducia dell'account in ogni regione.
- Viene creato lo strumento di analisi degli accessi inutilizzati di IAM Access Analyzer per l'account corrente.
- Viene creato l'analizzatore di accessi inutilizzati IAM Access Analyzer per l'organizzazione corrente.

Amazon Detective

- Detective è abilitato per tutti gli account dei membri.
- Detective è abilitato automaticamente per tutti gli account dei nuovi membri.
- Detective è abilitato per tutte le regioni.
- L'amministratore delegato di Detective è impostato sull'account Security Tooling.
- L'amministratore delegato CSPM di Detective and Security Hub è impostato sullo stesso account Security Tooling. GuardDuty
- Detective è integrato con Security Lake per l'archiviazione e l'analisi dei log non elaborati.
- Detective è integrato GuardDuty per l'ingestione dei risultati.
- Detective sta inserendo i log di controllo di Amazon EKS a scopo di analisi.
- Detective sta inserendo i log CSPM di Security Hub per l'analisi.

AWS Firewall Manager

- Le politiche di sicurezza di Firewall Manager sono impostate.
- L'amministratore delegato di Firewall Manager è impostato sull'account Security Tooling.
- AWS Config è abilitato come prerequisito.
- Più amministratori di Firewall Manager sono impostati con un ambito limitato per unità organizzativa, account e regione.

- Viene definita una politica AWS WAF di sicurezza Firewall Manager.
- Viene definita una politica di registrazione AWS WAF centralizzata di Firewall Manager.
- Viene definita una politica di sicurezza Firewall Manager Shield Advanced.
- Viene definita una politica di sicurezza del gruppo di sicurezza Firewall Manager.

Amazon Inspector

- Amazon Inspector è abilitato per tutti gli account dei membri.
- Amazon Inspector viene abilitato automaticamente per ogni nuovo account membro.
- L'amministratore delegato di Amazon Inspector è impostato sull'account Security Tooling.
- La scansione delle EC2 vulnerabilità di Amazon Inspector è abilitata.
- La scansione delle vulnerabilità delle immagini di Amazon Inspector ECR è abilitata.
- La scansione delle vulnerabilità della funzione e dei livelli di Amazon Inspector Lambda è abilitata.
- La scansione del codice Amazon Inspector Lambda è abilitata.
- La scansione di sicurezza del codice di Amazon Inspector è abilitata.

Amazon Macie

- Macie è abilitato per gli account membro applicabili.
- Macie è abilitato automaticamente per gli account dei nuovi membri applicabili.
- L'amministratore delegato di Macie è impostato sull'account Security Tooling.
- I risultati di Macie vengono esportati in un bucket S3 centrale nell'account Log Archive.
- I bucket S3 che memorizzano i risultati di Macie sono crittografati con una chiave gestita dal cliente.
- La politica e la politica di classificazione di Macie sono pubblicate su Security Hub CSPM.

Amazon Security Lake

- La configurazione dell'organizzazione di Security Lake è abilitata.
- L'amministratore delegato di Security Lake è impostato sull'account Security Tooling.
- La configurazione dell'organizzazione Security Lake è abilitata per gli account dei nuovi membri.

- L'account Security Tooling è configurato come abbonato all'accesso ai dati per condurre l'analisi dei log.
- L'account Security Tooling è configurato come abbonato alle interrogazioni di dati per condurre l'analisi dei log.
- Una fonte di log di CloudTrail gestione è abilitata per Security Lake in tutti gli account dei membri attivi o in alcuni account dei membri attivi.
- Una fonte di log di flusso VPC è abilitata per Security Lake in tutti gli account dei membri attivi o in alcuni account membri attivi.
- Una fonte di log Route 53 è abilitata per Security Lake in tutti gli account dei membri attivi o in alcuni account membri attivi.
- CloudTrail un evento di dati per una fonte di log S3 è abilitato per Security Lake in tutti gli account dei membri attivi o in alcuni account membri attivi.
- Un'origine del registro di esecuzione Lambda è abilitata per Security Lake in tutti gli account dei membri attivi o in alcuni account membri attivi.
- Una fonte di log di controllo Amazon EKS è abilitata per Security Lake in tutti gli account dei membri attivi o in alcuni account membri attivi.
- Un'origine del registro dei risultati di Security Hub è abilitata per Security Lake in tutti gli account dei membri attivi o in alcuni account membri attivi.
- Una fonte di AWS WAF registro è abilitata per Security Lake in tutti gli account dei membri attivi o in alcuni account membri attivi.
- Le code SQS di Security Lake nell'account amministratore delegato sono crittografate con una chiave gestita dal cliente.
- La coda di posta indesiderata di Security Lake SQS nell'account amministratore delegato è crittografata con una chiave gestita dal cliente.
- Il bucket Security Lake S3 è crittografato con una chiave gestita dal cliente.
- Il bucket Security Lake S3 ha una politica delle risorse che limita l'accesso diretto solo da parte di Security Lake.

AWS WAF

- Tutte le CloudFront distribuzioni sono associate a. AWS WAF
- Tutti i REST di Amazon API Gateway APIs sono associati a AWS WAF.

- Tutti gli Application Load Balancer sono associati a. AWS WAF
- Tutti i AWS AppSync GraphQL APIs sono associati a. AWS WAF
- Tutti i pool di utenti di Amazon Cognito sono associati a. AWS WAF
- Tutti i AWS App Runner servizi sono associati AWS WAF a.
- Tutte le Accesso verificato da AWS istanze sono associate AWS WAF a.
- Tutte le AWS Amplify applicazioni sono associate AWS WAF a.
- AWS WAF la registrazione è abilitata.
- AWS WAF i log sono centralizzati in un bucket S3 nell'account Log Archive.

AWS Shield Advanced

- L'abbonamento Shield Advanced è abilitato e impostato per il rinnovo automatico per tutti gli account delle applicazioni che dispongono di risorse rivolte al pubblico.
- Shield Advanced è configurato per tutte le CloudFront distribuzioni.
- Shield Advanced è configurato per tutti gli Application Load Balancer.
- Shield Advanced è configurato per tutti i Network Load Balancer.
- Shield Advanced è configurato per tutte le zone ospitate su Route 53.
- Shield Advanced è configurato per tutti gli indirizzi IP elastici.
- Shield Advanced è configurato per tutti gli acceleratori globali.
- CloudWatch gli allarmi sono configurati per CloudFront le risorse Route 53 protette da Shield Advanced.
- L'accesso allo Shield Response Team (SRT) è configurato.
- Il coinvolgimento proattivo Shield Advanced è abilitato.
- I contatti di coinvolgimento proattivo Shield Advanced sono configurati.
- Le risorse protette Shield Advanced hanno una AWS WAF regola personalizzata configurata.
- Le risorse protette Shield Advanced hanno la mitigazione automatica DDo S a livello di applicazione abilitata.

AWS Risposta agli incidenti di sicurezza

- AWS Security Incident Response è abilitato per l'intera AWS organizzazione.

- L'amministratore delegato AWS di Security Incident Response è impostato sull'account Security Tooling.
- Il flusso di lavoro di risposta proattiva e di valutazione degli avvisi è abilitato.
- AWS Le azioni di contenimento del Customer Incident Response Team (CIRT) sono autorizzate.

AWS Audit Manager

- Audit Manager è abilitato per tutti gli account dei membri.
- Audit Manager è abilitato automaticamente per gli account dei nuovi membri.
- L'amministratore delegato di Audit Manager è impostato sull'account Security Tooling.
- AWS Config è abilitato come prerequisito per Audit Manager.
- Per i dati archiviati in Audit Manager viene utilizzata una chiave gestita dal cliente.
- La destinazione predefinita del rapporto di valutazione è configurata.

Risorse IAM

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

Sebbene AWS Identity and Access Management (IAM) non sia un servizio incluso in un diagramma di architettura tradizionale, riguarda ogni aspetto dell' AWS organizzazione e. Account AWS Servizi AWS Non è possibile distribuirne alcuno Servizi AWS senza prima creare entità IAM e concedere le autorizzazioni. Una spiegazione completa di IAM non rientra nell'ambito di questo documento, ma questa sezione fornisce importanti riepiloghi delle raccomandazioni sulle migliori pratiche e indicazioni su risorse aggiuntive.

- Per le best practice IAM, consulta le best practice di sicurezza in IAM nella AWS documentazione, gli articoli IAM nel blog AWS sulla sicurezza e le presentazioni di AWS re:Invent.
- Il pilastro di sicurezza AWS Well-Architected delinea i passaggi chiave del processo di gestione delle autorizzazioni: definire i limiti delle autorizzazioni, concedere l'accesso con privilegi minimi, analizzare l'accesso pubblico e tra account, condividere le risorse in modo sicuro, ridurre continuamente le autorizzazioni e stabilire un processo di accesso di emergenza.
- La tabella seguente e le relative note di accompagnamento forniscono una panoramica di alto livello delle linee guida consigliate sui tipi di policy di autorizzazione IAM disponibili e su come utilizzarle nell'architettura di sicurezza. Per saperne di più, guarda il video AWS re:Invent 2020 sulla scelta del giusto mix di policy IAM.

Caso d'uso o policy	Effetto	Gestito da	Scopo	Riguarda	Influisce	Implementato in
Politiche di controllo del servizio () SCPs	Restrict	Team centrale, ad esempio il team di piattaforma o di	Guardrail, governance	Organizzazione, unità organizzativa, account	Tutti i responsabili dell'organizzazione, dell'unità organizza	Account di gestione dell'organizzazione [2]

		sicurezza [1]			tiva e degli account	
Politiche di controllo delle risorse (RCPs)	Restrict	Team centrale, ad esempio il team di piattaforma o di sicurezza [1]	Guardrail, governance	Organizzazione, unità organizzativa, account	Risorse negli account dei membri [12]	Account di gestione dell'organizzazione [2]
Politiche di automazione degli account di base (i ruoli IAM utilizzati dalla piattaforma per gestire un account)	Concedi e limita	Team centrale, ad esempio team di piattaforma, sicurezza o IAM [1]	Autorizzazioni per ruoli (di base) di automazione diversi dal carico di lavoro [3]	Account singolo [4]	Principi utilizzati dall'automazione all'interno di un account membro	Account dei membri
Politiche umane di base (i ruoli IAM che concedono agli utenti le autorizzazioni per svolgere il proprio lavoro)	Concedi e limita	Team centrale, ad esempio team di piattaforma, sicurezza o IAM [1]	Autorizzazioni per ruoli umani [5]	Account singolo [4]	Responsabili federati [5] e utenti IAM [6]	Account dei membri

Limiti delle autorizzazioni (autorizzazioni massime che uno sviluppatore autorizzato può assegnare a un altro responsabile)	Restrict	Team centrale, ad esempio team di piattaforma, sicurezza o IAM [1]	Guardrails per i ruoli applicativi (devono essere applicati)	Account singolo [4]	Ruoli individuali per un'applicazione o un carico di lavoro in questo account [7]	Account dei membri
Politiche relative ai ruoli delle macchine per le applicazioni (ruolo associato all'infrastruttura implementata dagli sviluppatori)	Concedi e limita	Delegato agli sviluppatori [8]	Autorizzazione per l'applicazione o il carico di lavoro [9]	Account singolo	Un intestatario di questo account	Account dei membri
Policy delle risorse	Concedi e limita	Delegato agli sviluppatori [8,10]	Autorizzazioni alle risorse	Account singolo	Un responsabile di un account [11]	Account dei membri

Gestione centralizzata degli utenti root	Concedi e limita	Team centrale, ad esempio team di piattaforma, sicurezza o IAM [1]	Gestisci centralmente gli utenti root degli account membri su larga scala	Organizzazione	Tutti gli utenti root negli account dei membri	Account di gestione dell'organizzazione, account amministratore delegato

Note dalla tabella:

1. Le aziende dispongono di molti team centralizzati (ad esempio team che si occupano di piattaforme cloud, addetti alle operazioni di sicurezza o di gestione delle identità e degli accessi) che si dividono le responsabilità di questi controlli indipendenti e sottopongono a revisione paritaria le rispettive politiche. Gli esempi riportati nella tabella sono segnaposto. Dovrete determinare la separazione delle mansioni più efficace per la vostra azienda.
2. Per utilizzarlo SCPs, è necessario abilitare tutte le funzionalità all'interno AWS Organizations.
3. In genere sono necessari ruoli e politiche di base comuni per consentire l'automazione, come le autorizzazioni per la pipeline, gli strumenti di distribuzione, gli strumenti di monitoraggio (ad esempio AWS Lambda e Regole di AWS Config) e altre autorizzazioni. Questa configurazione viene in genere fornita al momento del provisioning dell'account.
4. Sebbene riguardino una risorsa (ad esempio un ruolo o una politica) in un singolo account, possono essere replicati o distribuiti su più account utilizzando. AWS CloudFormation StackSets
5. Definisci un set base di ruoli umani e politiche di base da distribuire a tutti gli account dei membri da un team centrale (spesso durante il provisioning degli account). Gli esempi includono gli sviluppatori del team della piattaforma, del team IAM e dei team di controllo della sicurezza.
6. Utilizza la federazione delle identità (anziché gli utenti IAM locali) quando possibile.
7. I limiti delle autorizzazioni vengono utilizzati dagli amministratori delegati. Questa policy IAM definisce le autorizzazioni massime e sostituisce le altre politiche (incluse le `"*:*"` politiche che consentono tutte le azioni sulle risorse). I limiti delle autorizzazioni dovrebbero essere richiesti nelle politiche umane di base come condizione per creare ruoli (come i ruoli relativi alle prestazioni dei carichi di lavoro) e allegare politiche. Configurazioni aggiuntive come l'imposizione del SCPs limite delle autorizzazioni.

8. Ciò presuppone che siano stati implementati parapetti sufficienti (ad esempio, SCPs e limiti di autorizzazione).
9. Queste politiche opzionali potrebbero essere fornite durante il provisioning dell'account o come parte del processo di sviluppo dell'applicazione. L'autorizzazione a creare e allegare queste politiche sarà regolata dalle autorizzazioni dello sviluppatore dell'applicazione.
10. Oltre alle autorizzazioni degli account locali, un team centralizzato (come il team della piattaforma cloud o il team delle operazioni di sicurezza) spesso gestisce alcune politiche basate sulle risorse per consentire l'accesso tra più account per gestire gli account (ad esempio, per fornire l'accesso ai bucket S3 per la registrazione).
11. Una policy IAM basata sulle risorse può fare riferimento a qualsiasi principale di qualsiasi account per consentire o negare l'accesso alle sue risorse. Può anche fare riferimento a principi anonimi per consentire l'accesso pubblico.
12. RCPs si applicano alle risorse per un sottoinsieme di. Servizi AWS Per ulteriori informazioni, consulta Elenco di Servizi AWS tale supporto RCPs nella AWS Organizations documentazione.

Garantire che le identità IAM dispongano solo delle autorizzazioni necessarie per una serie di attività ben delineate è fondamentale per ridurre il rischio di abuso doloso o involontario delle autorizzazioni. La definizione e il mantenimento di un modello di privilegio minimo richiedono un piano deliberato per aggiornare, valutare e mitigare continuamente i privilegi in eccesso. Ecco alcuni consigli aggiuntivi per questo piano:

- Utilizza il modello di governance e la propensione al rischio consolidata della tua organizzazione per stabilire barriere e limiti di autorizzazione specifici.
- Implementa il privilegio minimo attraverso un processo iterativo continuo. Non si tratta di un esercizio da eseguire una sola volta.
- SCPs Da utilizzare per ridurre i rischi attuabili. Questi sono pensati per essere ampi guardrail, non controlli strettamente mirati.
- Utilizza i limiti delle autorizzazioni per delegare l'amministrazione di IAM in modo più sicuro.
  - Assicurati che gli amministratori delegati applichino la policy di confine IAM appropriata ai ruoli e agli utenti che creano.
- Come defense-in-depth approccio (in combinazione con le politiche basate sull'identità), utilizza politiche IAM basate sulle risorse per negare un ampio accesso alle risorse.

- Utilizza IAM access advisor AWS CloudTrail, IAM Access Analyzer e gli strumenti correlati per analizzare regolarmente l'utilizzo cronologico e le autorizzazioni concesse. Correggi immediatamente le ovvie sovraautorizzazioni.
- Se applicabile, assegna azioni generali a risorse specifiche anziché utilizzare un asterisco come carattere jolly per indicare tutte le risorse.
- Implementa un meccanismo per identificare, rivedere e approvare rapidamente le eccezioni alle policy IAM in base alle richieste.

Archivio di codice per esempi AWS SRA

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

Per aiutarti a iniziare a creare e implementare le linee guida contenute nella AWS SRA, questa guida è corredata da un repository Infrastructure as Code (IaC) all'indirizzo https://github.com/aws-samples/aws-security-reference-architecture-examples. Questo repository contiene codice per aiutare sviluppatori e ingegneri a implementare alcune delle linee guida e dei modelli di architettura presentati in questo documento. Questo codice è tratto dall'esperienza diretta dei consulenti dei Servizi AWS Professionali con i clienti. I modelli sono di natura generale: il loro obiettivo è illustrare un modello di implementazione piuttosto che fornire una soluzione completa. Le Servizio AWS configurazioni e le distribuzioni delle risorse sono volutamente molto restrittive. Potrebbe essere necessario modificare e personalizzare queste soluzioni per adattarle all'ambiente e alle esigenze di sicurezza.

L'archivio di codici AWS SRA fornisce esempi di codice con entrambe le opzioni di implementazione AWS CloudFormation e Terraform. I modelli di soluzione supportano due ambienti: uno richiede AWS Control Tower e l'altro lo utilizza senza. AWS Organizations AWS Control Tower Le soluzioni di questo repository che lo richiedono AWS Control Tower sono state implementate e testate all'interno di un AWS Control Tower ambiente utilizzando AWS CloudFormation and Customizations for AWS Control Tower (cFCT). Le soluzioni che non lo richiedono AWS Control Tower sono state testate all'interno di un AWS Organizations ambiente utilizzando. AWS CloudFormation La soluzione cFCT aiuta i clienti a configurare rapidamente un AWS ambiente sicuro e multi-account basato sulle AWS migliori pratiche. Aiuta a risparmiare tempo automatizzando la configurazione di un ambiente per l'esecuzione di carichi di lavoro sicuri e scalabili, implementando al contempo una linea di base di sicurezza iniziale attraverso la creazione di account e risorse. AWS Control Tower fornisce inoltre un ambiente di base per iniziare con un'architettura multi-account, la gestione delle identità e degli accessi, la governance, la sicurezza dei dati, la progettazione della rete e la registrazione. Le soluzioni nell'archivio AWS SRA forniscono configurazioni di sicurezza aggiuntive per implementare i modelli descritti in questo documento.

Di seguito è riportato un riepilogo delle soluzioni presenti nell'archivio SRA.AWS Ogni soluzione include un `README.md` file con i dettagli.

- La soluzione CloudTrail Organization crea un percorso organizzativo all'interno dell'account Org Management e delega l'amministrazione a un account membro come l'account Audit o Security Tooling. Questo percorso è crittografato con una chiave gestita dal cliente creata nell'account Security Tooling e invia i log a un bucket S3 nell'account Log Archive. Facoltativamente, gli eventi relativi ai dati possono essere abilitati per Amazon S3 AWS Lambda e le sue funzioni. Un percorso organizzativo registra gli eventi per tutti Account AWS i membri AWS dell'organizzazione, impedendo allo stesso tempo agli account dei membri di modificare le configurazioni.
- La soluzione GuardDuty Organization abilita Amazon GuardDuty delegando l'amministrazione all'account Security Tooling. Si configura GuardDuty all'interno dell'account Security Tooling per tutti gli account AWS aziendali esistenti e futuri. I GuardDuty risultati vengono inoltre crittografati con una chiave KMS e inviati a un bucket S3 nell'account Log Archive.
- La soluzione Security Hub CSPM Organization configura Security Hub CSPM delegando l'amministrazione all'account Security Tooling. Configura Security Hub CSPM all'interno dell'account Security Tooling per tutti gli account aziendali esistenti e futuri. AWS La soluzione fornisce anche parametri per la sincronizzazione degli standard di sicurezza abilitati su tutti gli account e le regioni, nonché per configurare un aggregatore di regioni all'interno dell'account Security Tooling. La centralizzazione di Security Hub CSPM all'interno dell'account Security Tooling offre una visione trasversale della conformità agli standard di sicurezza e dei risultati delle integrazioni sia di terze parti che di quelle di terze parti. Servizi AWS AWS Partner
- La soluzione Inspector configura Amazon Inspector all'interno dell'account amministratore delegato (Security Tooling) per tutti gli account e le regioni governate dell'organizzazione. AWS
- La soluzione Firewall Manager configura le politiche di AWS Firewall Manager sicurezza delegando l'amministrazione all'account Security Tooling e configurando Firewall Manager con una politica di gruppo di sicurezza e più politiche. AWS WAF La policy del gruppo di sicurezza richiede un gruppo di sicurezza massimo consentito all'interno di un VPC (esistente o creato dalla soluzione), che viene distribuito dalla soluzione.
- La soluzione Macie Organization abilita Amazon Macie delegando l'amministrazione all'account Security Tooling. Configura Macie all'interno dell'account Security Tooling per tutti gli account aziendali esistenti e futuri. AWS Macie è inoltre configurato per inviare i risultati della scoperta a un bucket S3 centrale crittografato con una chiave KMS.
- AWS Config:
  - La soluzione Config Aggregator configura un AWS Config aggregatore delegando l'amministrazione all'account Security Tooling. La soluzione configura quindi un AWS Config aggregatore all'interno dell'account Security Tooling per tutti gli account esistenti e futuri dell'organizzazione. AWS

  - La soluzione Conformance Pack Organization Rules viene Regole di AWS Config implementata delegando l'amministrazione all'account Security Tooling. Quindi crea un pacchetto di conformità dell'organizzazione all'interno dell'account amministratore delegato per tutti gli account esistenti e futuri dell'organizzazione. AWS La soluzione è configurata per implementare il modello di esempio del pacchetto di conformità Operational Best Practices for Encryption and Key Management.
  - La soluzione AWS Config Control Tower Management Account abilita AWS Config l'account di AWS Control Tower gestione e aggiorna di conseguenza l' AWS Config aggregatore all'interno dell'account Security Tooling. La soluzione utilizza il AWS Control Tower CloudFormation modello di abilitazione AWS Config come riferimento per garantire la coerenza con gli altri account dell' AWS organizzazione.
- IAM/
  - La soluzione Access Analyzer abilita IAM Access Analyzer delegando l'amministrazione all'account Security Tooling. Quindi configura un IAM Access Analyzer a livello di organizzazione all'interno dell'account Security Tooling per tutti gli account esistenti e futuri dell'organizzazione. AWS La soluzione implementa inoltre IAM Access Analyzer su tutti gli account membri e le regioni per supportare l'analisi delle autorizzazioni a livello di account.
  - La soluzione IAM Password Policy aggiorna la politica delle Account AWS password all'interno di tutti gli account di un'organizzazione. AWS La soluzione fornisce parametri per la configurazione delle impostazioni delle politiche relative alle password per aiutarti ad allinearti agli standard di conformità del settore.
- La soluzione EC2 Default EBS Encryption abilita la crittografia Amazon EBS predefinita a livello di account all'interno di ciascuna organizzazione Account AWS . Regione AWS AWS Applica la crittografia dei nuovi volumi e istantanee EBS che crei. Ad esempio, Amazon EBS crittografa i volumi EBS creati all'avvio di un'istanza e gli snapshot che copi da uno snapshot non crittografato.
- La soluzione S3 Block Account Public Access abilita le impostazioni a livello di account Amazon S3 all'interno Account AWS di ciascuna organizzazione. AWS La caratteristica di blocco dell'accesso pubblico di Amazon S3 fornisce le impostazioni per access point, bucket e account con cui è possibile gestire l'accesso pubblico alle risorse di Amazon S3. Per impostazione predefinita, nuovi bucket, access point e oggetti non consentono l'accesso pubblico. Tuttavia, gli utenti possono modificare le policy di bucket, le policy di access point o le autorizzazioni degli oggetti per consentire l'accesso pubblico. Le impostazioni di Amazon S3 Block Public Access hanno la precedenza su queste policy e autorizzazioni in modo da poter limitare l'accesso pubblico a queste risorse.

- La soluzione Detective Organization automatizza l'abilitazione di Amazon Detective delegando l'amministrazione a un account (come l'account Audit o Security Tooling) e configurando Detective per tutti gli account esistenti e futuri. AWS Organizations
- La soluzione Shield Advanced automatizza l'implementazione AWS Shield Advanced per fornire una protezione DDo S avanzata per le tue applicazioni su AWS.
- La soluzione AMI Bakery Organization aiuta ad automatizzare il processo di creazione e gestione di immagini Amazon Machine Image (AMI) standard e rinforzate. Ciò garantisce coerenza e sicurezza tra le AWS istanze e semplifica le attività di distribuzione e manutenzione.
- La soluzione Patch Manager aiuta a semplificare la gestione delle patch su più piattaforme. Account AWSÈ possibile utilizzare questa soluzione per aggiornare AWS Systems Manager Agent (SSM Agent) su tutte le istanze gestite e per scansionare e installare patch di sicurezza e correzioni di bug critiche e importanti su istanze con tag Windows e Linux. La soluzione configura anche l'impostazione Default Host Management Configuration per rilevare la creazione di nuove soluzioni Account AWS e distribuirle automaticamente su tali account.

Collaboratori

Autore principale:

- Avik Mukherjee, Senior Security S.A. AWS

Contributori:

- Jason Hurst, investigatore senior della sicurezza del AWS CIRT
- Abhishek Panday, Responsabile principale del prodotto, Tech AWS
- Itay Meller, specialista senior negli Stati Uniti AWS
- Jonathan, Principal Security VanKim AWS S.A.
- Josh Du Lac, AWS stratega della sicurezza aziendale
- James Thompson, architetto senior delle soluzioni AWS
- Jeremy Girven, Specialist SA AWS
- Rodney Underkoffler, Specialist Senior SA AWS
- Farhan Farooq, architetto senior delle soluzioni AWS
- Prashob Krishnan, responsabile tecnico degli account AWS
- Meg Peddada, consulente senior per la sicurezza AWS
- Ashwin Phadke, architetto senior delle soluzioni AWS
- Sowjanya Rajavaram, Senior Security SA AWS
- Tomek Jakubowski, consulente AWS senior
- Arun Thomas, architetto senior delle soluzioni AWS
- Ross Warren, architetto delle soluzioni di AWS prodotto
- Scott Conklin, consulente senior AWS
- Ilya Epshteyn, Senior Manager, Identity Solutions AWS
- Michael Haken, tecnico principale AWS
- Mehial Mendrin, consulente senior AWS
- Christopher Evensen, responsabile tecnico senior degli account AWS

Revisione:

- Eric Rose, AWS Principal Security S.A.
- Manoj Kumar, AWS consulente di consegna

Scrittura tecnica:

- Handan Selamoglu, scrittore tecnico senior AWS

Appendice: AWS servizi di sicurezza, identità e conformità

Influenza il futuro della AWS Security Reference Architecture (AWS SRA) rispondendo a un breve sondaggio.

Per un'introduzione o un aggiornamento, consulta Sicurezza, identità e conformità AWS sul AWS sito Web per un elenco di quelle Servizi AWS che ti aiutano a proteggere i carichi di lavoro e le applicazioni nel cloud. Questi servizi sono raggruppati in cinque categorie: protezione dei dati, gestione delle identità e degli accessi, protezione di reti e applicazioni, rilevamento delle minacce e monitoraggio continuo, conformità e privacy dei dati.

Protezione dei dati: AWS fornisce servizi che aiutano a proteggere dati, account e carichi di lavoro da accessi non autorizzati.

- Amazon Macie: scopri, classifica e proteggi i dati sensibili con funzionalità di sicurezza basate sull'apprendimento automatico.
- AWS KMS— Crea e controlla le chiavi utilizzate per crittografare i tuoi dati.
- AWS CloudHSM— Gestisci i tuoi moduli di sicurezza hardware (HSMs) in. Cloud AWS
- AWS Certificate Manager— Fornitura, gestione e distribuzione di SSL/TLS certificati da utilizzare con Servizi AWS.
- Gestione dei segreti AWS— Ruota, gestisci e recupera le credenziali del database, le chiavi API e altri segreti durante il loro ciclo di vita.

Gestione delle identità e degli accessi: i servizi di AWS identità consentono di gestire in modo sicuro identità, risorse e autorizzazioni su larga scala.

- IAM: controlla in modo sicuro l'accesso e le risorse. Servizi AWS
- IAM Identity Center: gestisci centralmente l'accesso SSO a più Account AWS applicazioni aziendali.
- Amazon Cognito: aggiungi la registrazione, l'accesso e il controllo degli accessi degli utenti alle tue applicazioni web e mobili.
- AWS Directory Service— Utilizzare Microsoft Active Directory gestito in Cloud AWS.
- AWS RAM— Condividi AWS le risorse in modo semplice e sicuro.

- AWS Organizations— Implementazione di una gestione basata su policy per più utenti. Account AWS
- Autorizzazioni Amazon Verified: gestisci autorizzazioni e autorizzazioni scalabili e dettagliate nelle tue applicazioni personalizzate.

Protezione di reti e applicazioni: queste categorie di servizi consentono di applicare politiche di sicurezza granulari nei punti di controllo della rete in tutta l'organizzazione. Servizi AWS consentono di ispezionare e filtrare il traffico per impedire l'accesso non autorizzato alle risorse ai confini a livello di host, di rete e di applicazione.

- AWS Shield— Proteggi le tue applicazioni web in esecuzione con la protezione S gestita. AWS DDo
- AWS WAF— Proteggi le tue applicazioni web dagli exploit web più comuni e garantisci disponibilità e sicurezza.
- AWS Firewall Manager— Configura e gestisci AWS WAF le regole per tutte Account AWS le applicazioni da una posizione centrale.
- AWS Systems Manager— Configura e gestisci Amazon EC2 e i sistemi locali per applicare patch al sistema operativo, creare immagini di sistema sicure e configurare sistemi operativi sicuri.
- Amazon VPC: fornisce una sezione logicamente isolata AWS in cui è possibile avviare AWS risorse in una rete virtuale definita dall'utente.
- AWS Network Firewall— Implementa le protezioni di rete essenziali per il tuo. VPCs
- Amazon Route 53 DNS Firewall: proteggi le tue richieste DNS in uscita dai tuoi. VPCs
- Accesso verificato da AWS— Fornisci un accesso sicuro alle tue applicazioni senza richiedere reti private virtuali (VPNs).
- Amazon VPC Lattice: semplifica la service-to-service connettività, la sicurezza e il monitoraggio.

Rilevamento delle minacce e monitoraggio continuo: i servizi di AWS monitoraggio e rilevamento forniscono indicazioni per aiutare a identificare potenziali incidenti di sicurezza all'interno del tuo ambiente. AWS

- AWS Security Hub CSPM— Visualizza e gestisci gli avvisi di sicurezza e automatizza i controlli di conformità da una posizione centrale.
- AWS Security Hub— Correla e arricchisci i risultati sulla sicurezza per dare priorità ai problemi di sicurezza critici per tutti i tuoi account e. Regioni AWS

- Amazon GuardDuty: proteggi i tuoi carichi di lavoro Account AWS e quelli di lavoro con il rilevamento intelligente delle minacce e il monitoraggio continuo.
- Amazon Inspector: automatizza le valutazioni di sicurezza per contribuire a migliorare la sicurezza e la conformità delle applicazioni su cui vengono distribuite. AWS
- AWS Config— Registra e valuta le configurazioni delle tue AWS risorse per consentire il controllo della conformità, il monitoraggio delle modifiche alle risorse e l'analisi della sicurezza.
- Regole di AWS Config— Crea regole che agiscano automaticamente in risposta ai cambiamenti dell'ambiente, ad esempio isolando le risorse, arricchendo gli eventi con dati aggiuntivi o ripristinando la configurazione a uno stato soddisfacente noto.
- AWS Security Incident Response— Automatizza la risposta, l'indagine e la correzione degli incidenti di sicurezza con playbook e flussi di lavoro predefiniti.
- AWS CloudTrail— Monitora l'attività degli utenti e l'utilizzo delle API per consentire la governance e il controllo operativo e dei rischi delle vostre attività. Account AWS
- Amazon Detective: analizza e visualizza i dati di sicurezza per individuare rapidamente la causa principale di potenziali problemi di sicurezza.
- AWS Lambda— Esegui codice senza dover fornire o gestire server, in modo da poter scalare la risposta programmata e automatizzata agli incidenti.

Conformità e privacy dei dati: AWS offre una visione completa dello stato di conformità e monitora continuamente l'ambiente utilizzando controlli di conformità automatizzati basati sulle AWS migliori pratiche e sugli standard di settore seguiti dall'azienda.

- AWS Artifact— Utilizza un portale self-service gratuito per accedere su richiesta ai report di AWS sicurezza e conformità e ad accordi online selezionati.
- AWS Audit Manager— Verifica continuamente AWS l'utilizzo per semplificare la valutazione del rischio e della conformità alle normative e agli standard di settore.

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
Ristrutturazione e aggiornamenti dei contenuti	• Sono state aggiunte linee guida per Security Hub e AWS Nitro Enclaves. • Ha ristrutturato l' AWS SRA per concentrarsi sull'architettura di base e ha spostato le sezioni di approfondimento in guide separate per la gestione delle identità, la sicurezza perimetrale, la cyber forensics, l'intelligenza artificiale generativa e l'IoT. • Linee guida esistenti aggiornate per includere dettagli aggiuntivi per AWS CloudTrail Amazon Detective, Amazon AWS Firewall Manager GuardDuty, IAM Access Analyzer, Amazon Security Lake e AWS Audit Manager. AWS Config AWS Shield Advanced	22 dicembre 2025
Aggiornamenti importanti	• Sono state aggiunte informazioni sulla nuova	29 agosto 2025

gestione centralizzata degli accessi degli utenti root IAM, sulle politiche di controllo delle risorse (RCPs) e sulle politiche dichiarative.

- Riferimenti CSPM di Security Hub aggiornati al nuovo Security Hub CSPM.
- Incluse nuove funzionalità di servizio per Amazon GuardDuty e Security Hub CSPM.
- È stata aggiunta una guida al AWS Security Incident Response servizio.
- Linee guida approfondite IAM aggiornate per includere VPC Lattice per machine-to-machine la gestione delle identità.
- Aggiunta una nuova guida approfondita: SRA for IoT.

Aggiunte e chiarimenti	• Nella sezione relativa all'account Security Tooling, sono state aggiornate le linee guida. AWS KMS • Nella sezione Gestione dell'identità del cliente, ha ampliato le informazioni sull'autorizzazione di API Gateway. • È stata aggiornata la sezione Generative AI per aggiungere una considera zione di progettazione per l'unità organizzativa e la progettazione dell'account. • Nella sezione AWS SRA code repository, sono state aggiunte informazioni sulla nuova soluzione Patch Management.	12 settembre 2024

Aggiornamenti importanti	• Sono state aggiunte due sezioni per una guida architettonica approfondita: AI generativa con Amazon Bedrock e gestione delle identità. • Sono state aggiornate le AWS Identity and Access Management Access Analyzer CloudFrontsezioni Amazon Detective, Amazon Inspector AWS Artifact,, AWS ConfigAmazon Security Lake e Amazon con nuove funzionalità di servizio. AWS Security Hub CSPM • È stata aggiornata la sezione del repository del codice AWS SRA per includere la nuova opzione di implementazione Terraform e l'aggiunta di soluzioni AWS Shield Advanced AMI Bakery.	7 giugno 2024

Aggiornamenti importanti	• Sono state aggiornate le sezioni Account di rete e Account dell'applicazione per aggiungere linee guida sull'architettura per Amazon Verified Permissions e Amazon VPC Lattice. Accesso verificato da AWS • Sono state aggiunte linee guida architettoniche approfondite basate sulla funzionalità di sicurezza. • Sono state aggiunte nuove linee guida sull' Servizi AWS utilizzo AI/ML per fornire migliori risultati di sicurezza. • Sono state aggiunte indicazioni su come pianifica re l'architettura di sicurezza in modo graduale.	4 novembre 2023
Aggiunta a Security Lake	Sono state aggiornate le sezioni dell'account Security Tooling e dell'account Log Archive per aggiungere linee guida di progettazione relative ad Amazon Security Lake.	22 settembre 2023

Aggiornamenti minori	• Linee guida esistenti aggiornate per rifletter e nuove Servizi AWS funzionalità e best practice. • Linee guida architetturali aggiornate per la AWS CloudTrail sicurezza perimetrale. AWS IAM Identity Center	10 maggio 2023
Sondaggio	È stato aggiunto un breve sondaggio per comprendere meglio come si utilizza l' AWS SRA nella propria organizza zione.	14 dicembre 2022
File di origine per i diagrammi dell'architettura di riferimento	Nella sezione AWS Security Reference Architecture, è stato aggiunto un file di download che fornisce i diagrammi di architettura per questa guida in formato modificabile. PowerPoint	17 novembre 2022
Aggiornamenti alla sezione Security Foundations	Nella sezione Security Foundations, sono state aggiornate le informazioni sui pilastri del Well-Architected Framework e sui principi di progettazione della sicurezza.	27 settembre 2022

Principali aggiunte e aggiornamenti	• Sono state aggiunte informazioni su come utilizzare l' AWS SRA e le principali linee guida di implementazione. • Sono state aggiunte linee guida sull'architettura per altre AWS Artifact applicazioni Servizi AWS come Amazon Inspector, AWS RAM Amazon Route 53,, AWS Control Tower AWS Audit Manager Directory Service, Amazon Cognito e Network Access Analyzer. • Linee guida esistenti aggiornate per rifletter e nuove Servizio AWS funzionalità e best practice.	25 luglio 2022
—	Pubblicazione iniziale	23 giugno 2021

AWS Glossario delle linee guida prescrittive

I seguenti sono termini di uso comune 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 del 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 di aggregazione

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 AIOps viene utilizzato nella strategia di AWS migrazione, 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 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 interrompere 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.

implementazione blu/verde

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 Cloud Adoption AWS 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.

CCoE

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 Servizio AWS riceva.

Centro di eccellenza 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 gli CCoE post 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 scalare l'adozione del cloud (ad esempio, creazione di una landing zone, definizione di una CCo E, 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 sul 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 oBitbucket Cloud. 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, Amazon SageMaker AI 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, compilazione, test, gestione temporanea e produzione del processo di rilascio del software. CI/CD viene comunemente descritto come una pipeline. CI/CD può aiutarvi ad automatizzare i processi, migliorare la produttività, migliorare la qualità del codice e velocizzare le consegne. 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.

MODIFICA

Vedi scambio elettronico di 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.

scambio elettronico di dati (EDI)

Lo scambio automatizzato di documenti aziendali tra organizzazioni. Per ulteriori informazioni, vedere Cos'è lo scambio elettronico di dati.

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 CI/CD pipeline, l'ambiente di produzione è l'ultimo ambiente di distribuzione.
- 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 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, consulta 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.

prompt con pochi scatti

Fornire a un LLM un numero limitato di esempi che dimostrino l'attività e il risultato desiderato prima di chiedergli di eseguire un'attività simile. Questa tecnica è un'applicazione dell'apprendimento contestuale, in cui i modelli imparano da esempi (immagini) incorporati nei prompt. I prompt con pochi passaggi possono essere efficaci per attività che richiedono una formattazione, un ragionamento o una conoscenza del dominio specifici. Vedi anche zero-shot prompting.

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.

FM

Vedi modello di base.

modello di fondazione (FM)

Una grande rete neurale di deep learning che si è addestrata su enormi set di dati generalizzati e non etichettati. FMs sono in grado di svolgere un'ampia varietà di attività generali, come comprendere il linguaggio, generare testo e immagini e conversare in linguaggio naturale. Per ulteriori informazioni, consulta Cosa sono i modelli Foundation.

G

IA generativa

Un sottoinsieme di modelli di intelligenza artificiale che sono stati addestrati su grandi quantità di dati e che possono utilizzare un semplice messaggio di testo per creare nuovi contenuti e artefatti, come immagini, video, testo e audio. Per ulteriori informazioni, consulta Cos'è l'IA generativa.

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.

immagine dorata

Un'istantanea di un sistema o di un software utilizzata come modello per distribuire nuove istanze di quel sistema o software. Ad esempio, nella produzione, un'immagine dorata può essere utilizzata per fornire software su più dispositivi e contribuire a migliorare la velocità, la scalabilità e la produttività nelle operazioni di produzione dei dispositivi.

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 alto livello che aiuta a governare le risorse, le politiche e la conformità tra le unità organizzative (). OUs 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 CSPM 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.

dati di blocco

Una parte di dati storici etichettati che viene trattenuta da un set di dati utilizzata per addestrare un modello di apprendimento automatico. È possibile utilizzare i dati di holdout per valutare le prestazioni del modello confrontando le previsioni del modello con i dati di holdout.

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, come 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

Vedi 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. La AWS Security Reference Architecture consiglia di configurare l'account di rete con funzionalità in entrata, in uscita e di ispezione VPCs 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.

IIoInternet delle cose industriale (T)

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, vedere Creazione di una strategia di trasformazione digitale per l'Internet of Things (IIoT) industriale.

VPC di ispezione

In un'architettura AWS multi-account, un VPC centralizzato che gestisce le ispezioni del traffico di rete tra VPCs (nello stesso o in modo diverso Regioni AWS), Internet e le reti locali. La AWS Security Reference Architecture consiglia di configurare l'account di rete con informazioni in entrata, in uscita e di ispezione VPCs 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, vedere Interpretabilità del modello 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.

modello linguistico di grandi dimensioni (LLM)

Un modello di intelligenza artificiale di deep learning preaddestrato su una grande quantità di dati. Un LLM può svolgere più attività, come rispondere a domande, riepilogare documenti, tradurre testo in altre lingue e completare frasi. Per ulteriori informazioni, consulta Cosa sono. LLMs

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.

LLM

Vedi modello linguistico di grandi dimensioni.

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

Servizi AWS 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 servizio piccolo e indipendente che comunica tramite canali ben definiti ed è in genere di proprietà di piccoli team autonomi. APIs 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 attraverso un'interfaccia ben definita utilizzando sistemi leggeri. APIs 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.

ORR

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. La AWS Security Reference Architecture consiglia di configurare l'account di rete con funzionalità in entrata, in uscita e di ispezione VPCs 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.

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`WHERE`. `true` `false`

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 di ingegneria dei sistemi che tiene conto della privacy durante l'intero processo di sviluppo.

zone ospitate private

Un contenitore che contiene informazioni su come desideri che Amazon Route 53 risponda alle query DNS per un dominio e i relativi sottodomini all'interno di uno o più. VPCs 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.

concatenamento rapido

Utilizzo dell'output di un prompt LLM come input per il prompt successivo per generare risposte migliori. Questa tecnica viene utilizzata per suddividere un'attività complessa in sottoattività o per perfezionare o espandere iterativamente una risposta preliminare. Aiuta a migliorare l'accuratezza e la pertinenza delle risposte di un modello e consente risultati più granulari e personalizzati.

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.

publish/subscribe (pub/sub)

Un modello 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).

RAG

Vedi Retrieval Augmented Generation.

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. Questo determina ciò che si considera 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.

Region

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 utilizzare Regioni AWS il proprio 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 alle interruzioni o di ripristinarle. 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.

Retrieval Augmented Generation (RAG)

Una tecnologia di intelligenza artificiale generativa in cui un LLM fa riferimento a una fonte di dati autorevole esterna alle sue fonti di dati di formazione prima di generare una risposta. Ad esempio, un modello RAG potrebbe eseguire una ricerca semantica nella knowledge base o nei dati personalizzati di un'organizzazione. Per ulteriori informazioni, consulta Cos'è il RAG.

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 obiettivo del punto di ripristino.

VERSO

Vedi 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 Console di gestione AWS 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 Gestione dei segreti AWS, 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.

sicurezza fin dalla progettazione

Un approccio di ingegneria dei sistemi che tiene conto della sicurezza durante l'intero processo di sviluppo.

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. Servizio AWS

Policy di controllo dei servizi (SCP)

Una politica che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in. AWS Organizations SCPs definire barriere o fissare limiti alle azioni che un amministratore può delegare a utenti o ruoli. È possibile utilizzarli SCPs 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 Servizio AWS. Puoi utilizzare l'endpoint per connetterti a livello di programmazione al servizio di destinazione. Per ulteriori informazioni, consulta Endpoint del Servizio AWS 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.

prompt di sistema

Una tecnica per fornire contesto, istruzioni o linee guida a un LLM per indirizzarne il comportamento. I prompt di sistema aiutano a impostare il contesto e stabilire regole per le interazioni con gli utenti.

T

tag

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 puoi utilizzare per interconnettere le tue reti VPCs e quelle locali. 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 VPCs che consente di indirizzare il traffico utilizzando 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 query 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.

prompt zero-shot

Fornire a un LLM le istruzioni per eseguire un'attività ma non esempi (immagini) che possano aiutarla. Il LLM deve utilizzare le sue conoscenze pre-addestrate per gestire l'attività. L'efficacia del prompt zero-shot dipende dalla complessità dell'attività e dalla qualità del prompt. Vedi anche few-shot prompting.

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.