Quadro per l'adozione del cloud AWS

Prospettiva di sicurezza

Giugno 2016

Note

Il presente documento è fornito a solo scopo informativo. In esso sono illustrate le attuali offerte di prodotti e le prassi di AWS alla data di pubblicazione del documento, offerte che sono soggette a modifica senza preavviso. È responsabilità dei clienti effettuare una propria valutazione indipendente delle informazioni contenute nel presente documento e dell'uso dei prodotti o dei servizi di AWS, ciascuno dei quali viene fornito "così com'è", senza garanzie di alcun tipo, né esplicite né implicite. Il presente documento non dà origine a garanzie, rappresentazioni, impegni contrattuali, condizioni o assicurazioni da parte di AWS, delle sue società affiliate, dei suoi fornitori o dei licenzianti. Le responsabilità di AWS nei confronti dei propri clienti sono definite dai contratti AWS e il presente documento non costituisce parte né modifica qualsivoglia contratto tra AWS e i suoi clienti.

Indice

Sintesi

Il whitepaper Quadro per l'adozione del cloud [1] (CAF) Amazon Web Services (AWS) fornisce indicazioni per coordinare i diversi ambiti delle organizzazioni che effettuano la migrazione al cloud computing. Le linee guida del framework CAF sono suddivise in vari argomenti di rilievo ai fini dell'implementazione dei sistemi IT basati su cloud. Tali argomenti di rilievo sono denominati prospettive; ogni prospettiva è ulteriormente suddivisa in componenti.È disponibile un whitepaper per ciascuna delle sette prospettive CAF.

Nel presente whitepaper viene trattata la Prospettiva di sicurezza, che riguarda in particolare l'integrazione delle linee guida e dei processi per i controlli di sicurezza esistenti, specifici per l'utilizzo di AWS nell'ambiente dell'utente.

Introduzione

La sicurezza è l'obiettivo principale di AWS. Tutti i clienti AWS traggono vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza. AWS e i suoi partner offrono centinaia di strumenti e caratteristiche che aiutano a raggiungere gli obiettivi di sicurezza in materia di visibilità, facilitazione degli audit, controllabilità e agilità. In questo modo si può avere tutta la sicurezza che serve, ma senza esborso anticipato di capitale e con costi operativi notevolmente inferiori.

Figura 1. Prospettiva di sicurezza di CAF AWS

L'obiettivo della Prospettiva di sicurezza è aiutare il cliente a strutturare la scelta e l'implementazione dei controlli più adatti alla propria organizzazione. Come illustra la figura 1, i componenti della Prospettiva di sicurezza organizzano i principi che contribuiscono alla trasformazione della cultura di sicurezza dell'organizzazione. Per ogni componente, il whitepaper esamina le azioni specifiche che si possono adottare e i mezzi per misurare i progressi compiuti:

- I controlli di **direzione** definiscono i modelli di governance, rischio e compliance in cui opererà l'ambiente.
- I controlli di **prevenzione** proteggono i carichi di lavoro e riducono le minacce e le vulnerabilità.
- I controlli di **individuazione** consentono di avere piena visibilità e trasparenza riguardo al funzionamento delle distribuzioni in AWS.
- I controlli di **reazione** consentono di porre rimedio ai possibili scostamenti rispetto alle baseline di sicurezza.

La sicurezza nel cloud è un elemento familiare. L'aumento dell'agilità e della capacità di compiere azioni più rapidamente, su più vasta scala e a un costo inferiore non rende inutili i principi consolidati della sicurezza informatica.

Dopo avere trattato i quattro componenti della Prospettiva di sicurezza, il whitepaper illustra le fasi che si possono intraprendere durante la transizione al cloud per garantire che l'ambiente mantenga un solido assetto di sicurezza:

- Definizione di una **strategia per la sicurezza** nel cloud. Quando si inizia la transizione, occorre esaminare i propri obiettivi organizzativi di business, tenere conto della gestione del rischio e valutare il livello di opportunità offerto dal cloud.
- Bisogna poi elaborare un **programma di sicurezza** per lo sviluppo e l'implementazione delle funzionalità di sicurezza, privacy, compliance e gestione del rischio. All'inizio può sembrare un compito titanico, pertanto è importante creare una struttura che permetta all'organizzazione di affrontare la sicurezza del cloud con un approccio olistico. L'implementazione deve permettere uno sviluppo iterativo, affinché le funzionalità maturino di pari passo con lo sviluppo dei programmi. In questo modo, il componente della sicurezza può essere un catalizzatore degli altri sforzi dell'organizzazione per l'adozione del cloud.

- È necessario sviluppare solide funzionalità per le operazioni di sicurezza che maturino e crescano costantemente. Il viaggio della sicurezza continua nel tempo. Consigliamo di unire il rigore operativo alla realizzazione di nuove funzionalità, affinché l'iterazione costante possa portare a un miglioramento continuo.

Vantaggi di AWS per la sicurezza

La sicurezza nel cloud, per AWS, è una priorità. In quanto cliente AWS, potrai trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

Un vantaggio del cloud AWS è che permette ai clienti di combinare scalabilità e innovazione, mantenendo allo stesso tempo un ambiente sicuro. I clienti pagano soltanto i servizi che utilizzano e in questo modo possono avere la sicurezza di cui hanno bisogno, ma senza spese anticipate e a un costo inferiore rispetto all'ambiente in locale.

Questa sezione esamina alcuni dei vantaggi per la sicurezza offerti dalla piattaforma AWS.

Progettata per la sicurezza

L'infrastruttura del cloud AWS è gestita nei data center di AWS ed è progettata per soddisfare i requisiti dei clienti più attenti alla sicurezza. L'infrastruttura di AWS è stata progettata per offrire un'alta disponibilità e implementare protezioni solide a tutela della privacy dei clienti. Tutti i dati sono memorizzati in data center AWS protetti. I firewall di rete integrati in Amazon VPC e le funzionalità dei firewall per le applicazioni Web in AWS WAF consentono di creare reti private e di controllare gli accessi a istanze e applicazioni.

Quando si distribuiscono sistemi nel cloud AWS, AWS dà il proprio contributo condividendo le responsabilità di sicurezza con il cliente. AWS progetta l'infrastruttura sottostante sulla base di principi di progettazione sicuri e i clienti hanno la possibilità di implementare la propria architettura di sicurezza per i carichi di lavoro distribuiti in AWS.

Elevata automazione

AWS realizza gli strumenti di sicurezza avendo ben chiaro il loro scopo e li personalizza per adattarli all'ambiente, alle dimensioni e ai requisiti globali unici del cliente. La realizzazione degli strumenti di sicurezza in tutti i loro elementi permette ad AWS di automatizzare molte delle attività di routine che normalmente assorbono il tempo degli esperti di sicurezza. In questo modo, gli esperti di sicurezza di AWS possono trascorrere più tempo a occuparsi delle misure necessarie a rafforzare la sicurezza dell'ambiente cloud AWS del cliente. I clienti, inoltre, possono automatizzare le funzioni di progettazione e gestione della sicurezza grazie a un set completo di API e strumenti. Le funzioni di gestione dell'identità, sicurezza della rete, protezione dei dati e monitoraggio possono essere interamente automatizzate e distribuite con l'ausilio di metodi di sviluppo software diffusi di cui il cliente già dispone.

I clienti adottano un approccio automatizzato per affrontare i problemi di sicurezza. Quando si utilizzano i servizi AWS per l'automazione, invece di chiedere ai dipendenti di monitorare la posizione di sicurezza, il sistema diventa in grado di monitorare, esaminare e avviare una risposta.

Alta disponibilità

AWS crea i propri data center in più regioni geografiche. All'interno delle regioni, esistono varie zone di disponibilità che garantiscono la flessibilità. AWS progetta i data center con un eccesso di larghezza di banda e in questo modo, se si verifica una perturbazione importante, è disponibile capacità sufficiente per effettuare il bilanciamento del carico del traffico e instradarlo verso i siti restanti, riducendo al minimo l'impatto sui clienti. I clienti possono inoltre sfruttare l'esistenza di più regioni e zone di disponibilità per creare applicazioni molto resilienti a un costo estremamente basso, per replicare ed effettuare il backup dei dati facilmente e per implementare controlli di sicurezza coerenti in tutta l'azienda.

Altamente accreditato

Gli ambienti AWS sono sottoposti a controlli continui e certificati da entità di controllo in tutto il mondo. Questo significa che alcuni aspetti di compliance del cliente sono già soddisfatti. Per maggiori informazioni sulla normativa e gli standard di sicurezza a cui AWS è conforme, vedere la pagina Web AWS Cloud Compliance[2]. Per aiutare i clienti a soddisfare normative e standard di sicurezza specifici di enti governativi, di settore e aziendali, AWS fornisce certificazioni che descrivono in che modo l'infrastruttura del cloud AWS soddisfa i requisiti di un lungo elenco di standard di sicurezza globali. È possibile ottenere i report di

compliance disponibili contattando il proprio rappresentante per gli account AWS. I clienti "ereditano" molti controlli gestiti da AWS nei propri programmi di compliance e certificazione, con conseguente riduzione dei costi di esecuzione e gestione dei controlli di sicurezza, oltre alla possibilità di gestire, di fatto, i controlli da soli. Grazie alle solide basi esistenti, il cliente è libero di ottimizzare la sicurezza dei propri carichi di lavoro, per garantire agilità, flessibilità e scalabilità.

La parte restante del whitepaper presenta ciascuno dei componenti della Prospettiva di sicurezza. Si possono utilizzare i componenti per esaminare gli obiettivi di sicurezza che devono essere raggiunti per concludere con successo la transizione al cloud.

Componente di indicazione

Il componente di indicazione della Prospettiva di sicurezza AWS fornisce linee guida per la pianificazione dell'approccio di sicurezza durante la migrazione ad AWS. L'elemento chiave della pianificazione efficace è la definizione delle linee guida da fornire alle persone che implementano e gestiscono l'ambiente di sicurezza. Le informazioni devono fornire un'indicazione sufficiente per stabilire i controlli necessari e le relative modalità di gestione. Le aree iniziali da prendere in considerazione includono:

- **Governance degli account**—Indirizza l'organizzazione alla creazione di un processo e di procedure per la gestione degli account AWS. Le aree da definire includono le modalità di raccolta e gestione degli inventari degli account, l'identificazione dei contratti e delle modifiche in essere e i criteri da utilizzare all'atto della creazione di un account AWS. Sviluppa un processo per la creazione degli account in modo coerente, per garantire che tutte le impostazioni iniziali siano idonee e che sia definita una titolarità chiara.
- **Informazioni sulla titolarità degli account e sui contatti**—Definisci un modello di governance idoneo per gli account AWS utilizzabile nell'intera organizzazione e pianifica il modo in cui le informazioni di contatto sono gestite per ciascun account. Si può valutare la creazione di account AWS collegati agli elenchi di distribuzione di posta elettronica, invece che a un singolo indirizzo e-mail. In questo modo un gruppo di persone può monitorare e reagire alle informazioni di AWS riguardo all'attività dell'account. Così si garantisce, inoltre, flessibilità in caso di avvicendamento del personale interno e si dispone di una modalità di assegnazione della responsabilità della sicurezza. Indica il team di sicurezza come punto di contatto per la sicurezza al

fine di accelerare le comunicazioni time-sensitive.

- **Quadro di controllo**—Definisci o applica un quadro di controllo conforme agli standard di settore e stabilisci se ti occorrono modifiche o aggiunte per integrare i servizi AWS ai livelli di sicurezza previsti. Esegui una mappatura della compliance per stabilire in che modo i requisiti di compliance e i controlli di sicurezza riflettono l'utilizzo dei servizi AWS.
- **Titolarità dei controlli**—Consulta le informazioni relative al Modello AWS di Responsabilità condivisa[3] nel sito Web di AWS per stabilire se è opportuno apportare modifiche alla titolarità dei controlli. Esamina e aggiorna la matrice di Responsibility Assignment (grafico RACI) per includere la titolarità dei controlli presenti nell'ambiente AWS.
- **Classificazione dei dati**—Esamina le attuali classificazioni dei dati e stabilisci in che modo tali classificazioni saranno gestite nell'ambiente AWS e quali controlli saranno opportuni.
- **Gestione delle modifiche e degli asset**—Stabilisci in che modo la gestione delle modifiche e la gestione degli asset devono essere eseguite in AWS. Crea un mezzo per stabilire quali sono gli asset esistenti, per che cosa sono utilizzati i sistemi e in che modo i sistemi saranno gestiti in sicurezza. Questi aspetti possono essere integrati al database esistente di gestione delle configurazioni (CMDB). Valuta la possibilità di creare una prassi per la denominazione e il tagging, che consenta di effettuare l'identificazione e la gestione al livello di sicurezza richiesto. Puoi utilizzare questo approccio per definire e tenere traccia dei metadata che consentono l'identificazione e il controllo.
- **Ubicazione dei dati**—Esamina i criteri relativi all'ubicazione dei dati per stabilire quali controlli occorreranno per gestire la configurazione e l'utilizzo dei servizi AWS tra le varie regioni. Sono i clienti di AWS a scegliere in quale regione o in quali regioni debbano essere immagazzinati i loro dati. Ciò permette agli utenti con specifiche esigenze geografiche di stabilire gli ambienti in una località a loro scelta. I clienti possono riprodurre i contenuti ed eseguirne il backup in diverse regioni; tuttavia AWS non sposta i contenuti del cliente dalla regione che lo stesso ha scelto.
- **Accesso con privilegio minimo**—Crea una cultura della sicurezza aziendale basata sul principio del privilegio minimo e sull'autenticazione a due fattori. Implementa protocolli di protezione degli accessi a credenziali sensibili e i materiali chiave associati a ogni account AWS. Stabilisci aspettative circa le modalità di delega dell'autorità fino ai tecnici software, al personale operativo e alle altre funzioni lavorative coinvolte nell'adozione del cloud.

- **Playbook e runbook relativi alle operazioni di sicurezza**—Definisci i tuoi pattern di sicurezza per creare guardrail duraturi a cui l'organizzazione possa fare riferimento nel tempo. Implementa i play attraverso l'automazione come runbook; documenta gli interventi human-in- the-loop come opportuno.

Considerazioni

- **Crea** un modello di responsabilità condivisa AWS su misura per il tuo ecosistema.
- **Usa** l'autenticazione a due fattori come parte di un meccanismo di protezione per tutti i soggetti del tuo account.
- **Promuovi** una cultura di titolarità della sicurezza per i team delle applicazioni.
- **Estendi** il tuo modello di classificazione dei dati in modo da includere servizi in AWS.
- **Integra** gli obiettivi e le funzioni lavorative dei team di sviluppatori, di gestione e di sicurezza.
- **Valuta** la possibilità di creare una strategia per denominare e tenere traccia degli account utilizzati per gestire i servizi in AWS.
- **Centralizza** gli elenchi telefonici e di distribuzione della posta elettronica affinché i team possano essere monitorati.

Componente di prevenzione

Il componente di prevenzione della Prospettiva di sicurezza AWS fornisce linee guida per implementare l'infrastruttura di sicurezza con AWS e all'interno della tua organizzazione.
La chiave per implementare l'insieme più adatto di controlli è consentire ai team di sicurezza di acquisire la fiducia e la capacità di cui hanno bisogno per sviluppare le competenze di automazione e distribuzione necessarie a proteggere l'impresa nell'ambiente agile e scalabile offerto da AWS.

Utilizza il componente di indicazione per stabilire quali controlli e linee guida ti occorrono e successivamente utilizza il componente di prevenzione per decidere come gestire i controlli in modo efficiente. AWS fornisce regolarmente linee guida relative a best practice per l'utilizzo dei servizi AWS e modelli di distribuzione dei carichi di lavoro utilizzabili come punti di riferimento per l'implementazione dei controlli. Visita il Centro di Sicurezza AWS, il blog e il summit AWS più recente e consulta i video sul monitoraggio presentati alla conferenza re:Invent.

Valuta le seguenti aree per stabilire le eventuali modifiche da apportare alle architetture e alle prassi di sicurezza attualmente presenti. In questo modo disporrai di una strategia pianificata e corretta per l'adozione di AWS.

- **Identità e accesso**—Integra l'uso di AWS nel ciclo di vita della forza lavoro dell'organizzazione, oltre che nelle fonti di autenticazione e autorizzazione. Crea policy e ruoli fine-grained associati agli utenti e ai gruppi idonei. Crea guardrail che consentano le modifiche importanti solo attraverso l'automazione e impediscano modifiche indesiderate oppure le annullino automaticamente. Queste fasi ridurranno l'accesso umano ai sistemi e ai dati di produzione.
- **Protezione dell'infrastruttura**—Implementa una baseline di sicurezza comprensiva di trust boundary, configurazione e manutenzione del sistema di sicurezza (ad es. protezione e patch) e altri punti idonei di applicazione delle policy (ad es. gruppi di sicurezza, AWS WAF, Amazon API Gateway) per soddisfare le esigenze che hai identificato con l'ausilio del componente di indicazione.
  - **Protezione dei dati**—Utilizza le tutele più adatte per proteggere i dati in transito e inattivi. Le tutele includono i controlli di accesso fine-grained sugli oggetti, la creazione e il controllo delle chiavi di crittografia utilizzate per crittografare i dati, la scelta dei metodi di crittografia o tokenizzazione più adatti, la convalida dell'integrità e un'idonea conservazione dei dati.

Considerazioni

- **Tratta** la sicurezza come un codice che ti consente di distribuire e convalidare l'infrastruttura di sicurezza per ottenere la scalabilità e l'agilità necessarie a proteggere l'organizzazione.
- **Crea** guardrail, impostazioni predefinite intelligenti e offri i modelli e le best practice come codice.
- **Crea** servizi di sicurezza che l'organizzazione possa utilizzare per funzioni di sicurezza altamente ripetitive o particolarmente sensibili.
- **Definisci** i soggetti e poi crea lo storyboard della loro esperienza di interazione con i servizi AWS.
- **Utilizza** lo strumento AWS Trusted Advisor per valutare in maniera continuativa il tuo assetto di sicurezza in AWS e considera la possibilità di impiegare AWS Well Architected Review.
- **Definisci** una baseline di sicurezza minima realizzabile ed effettua iterazioni continue per alzare le aspettative di qualità per i carichi di lavoro che proteggi.

Componente di individuazione

Il componente di individuazione della Prospettiva di sicurezza di AWS CAF fornisce linee guida per ottenere visibilità sull'assetto di sicurezza della tua organizzazione. Utilizzando servizi come AWS CloudTrail, log specifici per i servizi e i valori restituiti da API/CLI è possibile ottenere una grande quantità di dati e informazioni. Grazie all'integrazione di tali informazioni in una piattaforma scalabile per la gestione e il monitoraggio dei registri, la gestione degli eventi, i test e l'inventario/audit ti forniranno la trasparenza e l'agilità operativa che ti occorrono per poter considerare sicure le tue operazioni.

- **Logging e monitoraggio**—AWS fornisce il logging nativo e servizi utilizzabili per fornire maggiore visibilità, pressoché in tempo reale, per le occorrenza nell'ambiente AWS. Puoi utilizzare questi strumenti per integrarti con le soluzioni di logging e monitoraggio esistenti. Integra in profondità l'output delle fonti di logging e monitoraggio nel flusso di lavoro dell'organizzazione IT, per una risoluzione end-to-end dell'attività correlata alla sicurezza.
- **Test sicurezza**—Esegui test sull'ambiente AWS per assicurarti che gli standard di sicurezza definiti siano soddisfatti. Grazie ai test effettuati per stabilite se i sistemi reagiranno come previsto a determinati eventi, ti preparerai meglio ad affrontare gli eventi reali. Tra gli esempi di test di sicurezza si possono menzionare la scansione delle vulnerabilità, il test di intrusione e la fault injection per dimostrare il rispetto degli standard. L'obiettivo è accertare se il tuo controllo reagirà come previsto.
- **Inventario degli asset**—La conoscenza di quali carichi di lavoro hai distribuito e reso operativi permetterà di monitorare e garantire l'operatività dell'ambiente ai livelli di governance della sicurezza previsti e prescritti dagli standard di sicurezza.
- **Rilevazione delle modifiche**—Per poter fare affidamento su una baseline sicura di controlli preventivi, è anche necessario sapere quando tali controlli cambiano. Implementa misure per identificare l'eventuale scostamento tra la configurazione di sicurezza e lo stato attuale.

Considerazioni

- **Stabilisci** quali informazioni di logging relative all'ambiente AWS desideri acquisire, monitorare e analizzare.
- **Stabilisci** in che modo l'attuale funzionalità di business del SOC (Security Operations Center) integrerà il monitoraggio e la gestione della sicurezza di AWS nelle prassi esistenti.
- **Esegui** in maniera continuativa scansioni delle vulnerabilità e test di intrusione secondo le procedure previste da AWS.

Componente di reazione

Il componente di reazione della Prospettiva di sicurezza di AWS CAF fornisce linee guida per la parte dell'assetto di sicurezza della tua organizzazione che riguarda la reazione. Con l'integrazione dell'ambiente AWS nell'assetto di sicurezza esistente e con la successiva preparazione e simulazione di azioni che richiedono una reazione, sarai meglio preparato a reagire agli eventi imprevisti quando si verificano.

Attraverso la risposta agli eventi imprevisti e il ripristino automatizzati e alla capacità di migrare parti del disaster recovery, è possibile spostare l'attenzione prioritaria del team di sicurezza dalla reazione all'indagine scientifica e all'analisi delle cause sottostanti. Alcuni degli aspetti da tenere in considerazione nella fase di adattamento dell'assetto di sicurezza sono:

- **Risposta agli eventi imprevisti**—Durante un evento imprevisto, il contenimento dell'evento e il ritorno a uno stato corretto noto sono elementi importanti di un piano di risposta. Ad esempio, l'automazione di aspetti delle funzioni che utilizzano le regole di AWS Config e i responder script di AWS Lambda ti consente di adeguare la reazione alle velocità di Internet. Esamina i processi di reazione agli eventi imprevisti che si sono verificati e stabilisci se e come la reazione e il ripristino automatizzati diventeranno operativi e gestiti per gli asset AWS. Le funzioni del Security Operations Center dovrebbero essere strettamente integrate con le API di AWS per essere quanto più reattive possibile. In questo modo si ottiene la funzione di monitoraggio e gestione della sicurezza per l'adozione del cloud AWS.
- **Simulazioni di reazioni agli eventi imprevisti di sicurezza**—Attraverso la simulazione degli eventi, puoi convalidare che i controlli e i processi che hai implementato reagiscono come previsto. Utilizzando questo approccio, puoi stabilire se sei in grado di reagire ed effettuare il ripristino in modo efficace al verificarsi di eventi imprevisti.
- **Informatica forense**—Nella maggior parte dei casi, gli strumenti forensi di cui disponi funzioneranno nell'ambiente AWS. I team forensi trarranno vantaggio dalla distribuzione automatizzata degli strumenti tra le diverse regioni e dalla capacità di raccogliere rapidamente volumi elevati di dati, con il minimo attrito, utilizzando gli stessi servizi efficaci e scalabili su cui sono realizzate le applicazioni business-critical, come Amazon Simple Storage Service (S3), Amazon Elastic Block Store (EBS), Amazon Kinesis, Amazon DynamoDB, Amazon Relational Database Service (RDS), Amazon RedShift e Amazon Elastic Compute Cloud (EC2).

Considerazioni

- **Aggiorna** i processi di reazione agli eventi imprevisti affinché tengano conto dell'ambiente AWS.
- **Utilizza** i servizi AWS per preparare, in un'ottica forense, le tue distribuzioni, attraverso l'automazione e la scelta delle caratteristiche.
- **Automatizza** la risposta per garantire solidità e scalabilità.
- **Utilizza** i servizi AWS per la raccolta e l'analisi dei dati a supporto di un'indagine.
- **Convalida** la tua capacità di reazione agli eventi imprevisti attraverso simulazioni delle reazioni agli eventi imprevisti di sicurezza.

Il viaggio da compiere – Definizione di una strategia

Esamina la strategia di sicurezza attuale per stabilire se alcune parti di essa trarrebbero vantaggio da una modifica, nel quadro di un'iniziativa di adozione del cloud. Effettua la mappatura della strategia di adozione del cloud AWS sulla base del livello di rischio che la tua azienda è disposta ad accettare, dell'approccio adottato per raggiungere gli obiettivi normativi e di compliance, nonché delle definizioni di quello che deve essere protetto, e come. Nella tabella 1 è illustrato un esempio di strategia di sicurezza che enuncia una serie di principi, i quali sono poi mappati a iniziative specifiche e flussi di lavoro.

Principio	Azioni di esempio
Infrastruttura come codice.	Rafforza le competenze del team di sicurezza nel campo della codifica e dell'automazione; passa a DevSecOps.
Progetta guardrail, non gate.	Favorisci l'adozione di un comportamento corretto.
Usa il cloud per proteggere il cloud.	Realizza, rendi operativi e gestisci gli strumenti di sicurezza nel cloud.
Mantieniti aggiornato; esegui le attività in sicurezza.	Adotta nuove caratteristiche di sicurezza; applica le patch ed effettua sostituzioni frequenti.
Riduci l'affidamento sull'accesso persistente.	Definisci un catalogo di ruoli; automatizza KMI tramite il servizio Secrets.
Visibilità totale.	Aggrega i log di AWS e i metadata con log dell'OS e delle app.
Informazioni approfondite.	Implementa un data warehouse della sicurezza con BI e analisi.
Risposta agli eventi imprevisti (IR) scalabile.	Aggiorna la procedura operativa standard (SOP) per la reazione agli eventi imprevisti e gli aspetti forensi per il quadro di responsabilità condivisa.
Riparazione automatica.	Automatizza la correzione e il ripristino a uno stato corretto noto.

Tabella 1. Esempio di strategia di sicurezza

Con la progressiva evoluzione della tua strategia, vorrai iniziare a effettuare iterazioni sulla base dei tuoi framework di sicurezza di terze parti e dei requisiti di sicurezza dell'organizzazione e avviare l'integrazione in un framework di gestione del rischio che ti guidi durante la transizione ad AWS. Una prassi spesso efficace

consiste nel far evolvere la mappatura della compliance di pari passo con il miglioramento della comprensione delle esigenze dei carichi di lavoro nel cloud e delle funzionalità di sicurezza offerte da AWS.

Un altro elemento fondamentale della tua strategia è la mappatura del modello di responsabilità condivisa specifico per il tuo ecosistema. Oltre alla macrorelazione che condividi con AWS, vorrai esplorare le responsabilità organizzative condivise internamente insieme a quelle che assegni ai partner. Le aziende possono suddividere il modello di responsabilità condivisa in tre aree principali: un framework di controllo; un modello RACI (Responsible, Accountable, Consulted, Informed) e un registro dei rischi. Il framework di controllo descrive come ci si aspetta che funzionino gli aspetti di sicurezza dell'azienda e quali controlli saranno implementati per gestire il rischio. Puoi utilizzare il modello RACI per identificare e assegnare a una persona la responsabilità dei controlli nel framework. Infine, puoi utilizzare un registro dei rischi per acquisire i controlli privi di un'idonea titolarità. Assegna la priorità ai rischi residui identificati, allineando il loro trattamento ai nuovi flussi di lavoro e alle iniziative poste in essere per risolverli.

Mentre esegui la mappatura di queste responsabilità condivise, puoi aspettarti di trovare nuove opportunità per automatizzare le operazioni e migliorare il flusso di lavoro tra soggetti fondamentali della community di sicurezza, compliance e gestione del rischio. La figura 2 mostra un esempio di modello di responsabilità condivisa estesa.

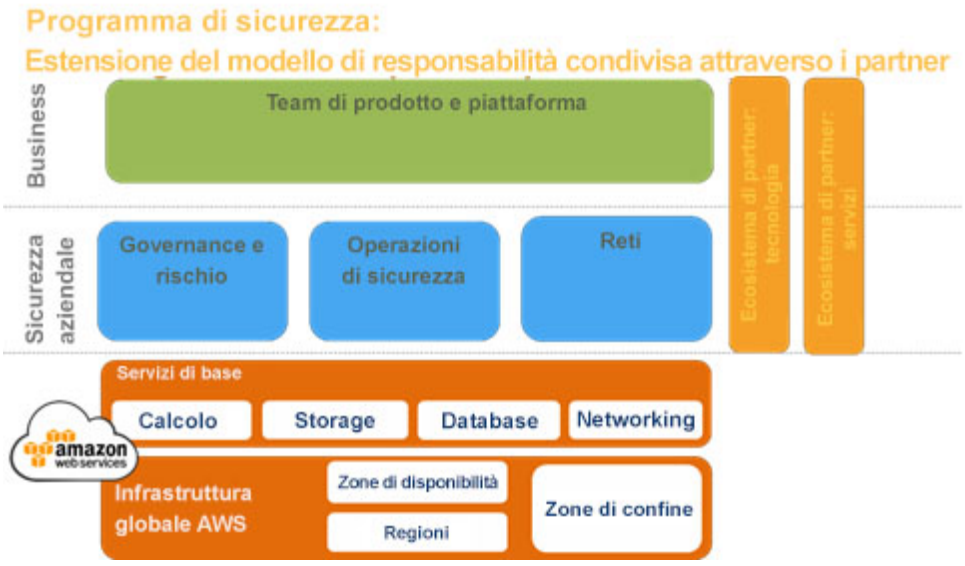

Figura 2. Esempio di modello di responsabilità condivisa

Considerazioni

- **Crea** una strategia su misura che integri il tuo approccio organizzativo riguardo all'implementazione della sicurezza nel cloud.
- **Valorizza** l'automazione quale tema sottostante di tutta la tua strategia.
- **Comunica** chiaramente, per prima cosa, il tuo approccio nei confronti del cloud.
- **Promuovi** l'agilità e la flessibilità attraverso la definizione di guardrail.
- **Considera** la strategia un breve esercizio che definisce l'approccio della tua organizzazione riguardo alla sicurezza delle informazioni nel cloud.
- **Effettua** rapidamente le iterazioni mentre definisci i contenuti della strategia. Il tuo obiettivo è disporre di una serie di principi guida che facciano avanzare lo sforzo principale: la strategia non è fine a se stessa. Muoviti velocemente e mostra disponibilità ad adattarti ed evolvere.
- **Definisci** principi strategici che veicoleranno la cultura della sicurezza che vuoi implementare e che saranno alla base delle decisioni progettuali che adotterai, invece di una strategia che preveda soluzioni specifiche.

Il viaggio da compiere – Elaborazione di un programma

Definita la strategia, è ora di mettere in pratica e avviare l'implementazione che trasformerà la tua organizzazione di sicurezza e garantirà una transizione sicura verso il cloud. Sebbene esista una vasta scelta di opzioni e caratteristiche, l'implementazione non dovrebbe essere uno sforzo prolungato. Questo processo di progettazione e implementazione delle modalità di interazione e integrazione delle diverse funzionalità rappresenta un'opportunità per acquisire rapidamente familiarità e imparare come ripetere i progetti per soddisfare al meglio i tuoi requisiti. Potrai imparare rapidamente dall'implementazione effettiva e successivamente adattarti ed evolvere adottando piccole modifiche mentre impari.

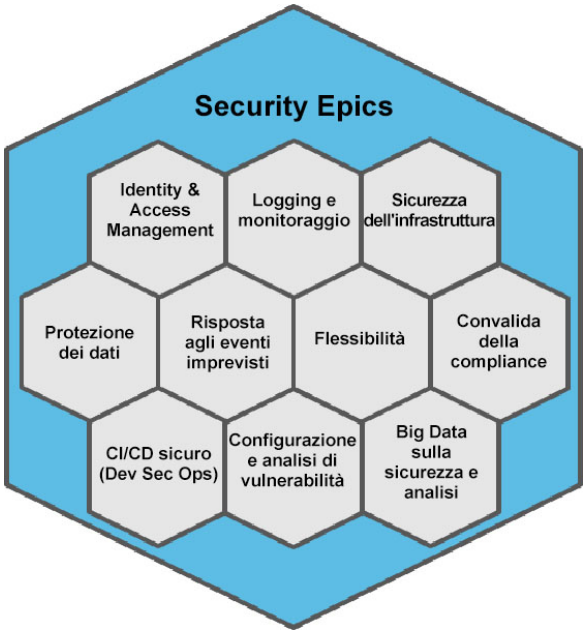

Figura 3. AWS CAF Security Epics

Come aiuto per l'implementazione, puoi utilizzare CAF Security Epics. (Si veda la figura 3). Security Epics è costituito da un gruppo di user story (casi d'uso e casi d'abuso) che puoi utilizzare durante gli sprint. Ognuno di questi gruppi ha più iterazioni per affrontare requisiti e layer di efficienza sempre più complessi. Sebbene consigliamo il ricorso all'agilità, i Security Epics possono essere anche considerati un flusso di lavoro generale o argomenti che aiutano ad assegnare la priorità e a strutturare la distribuzione utilizzando qualunque altro framework. Una delle strutture proposte è costituita dai seguenti 10 Security Epics (figura 4) che ti guideranno nell'implementazione.

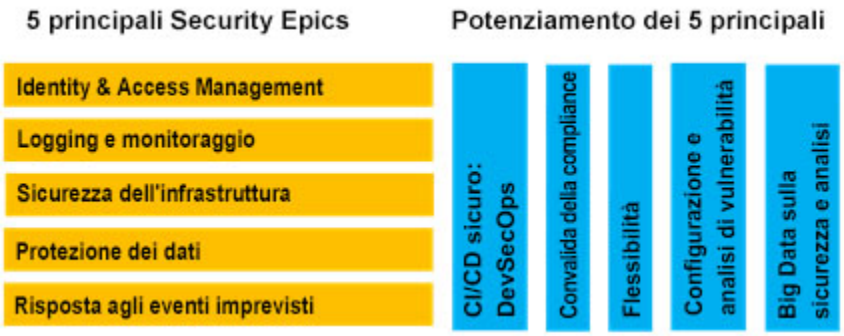

Figura 4. 10 AWS Security Epics

I cinque principali

I cinque seguenti Security Epics sono le principali categorie di controlli e funzionalità che dovresti tenere in considerazione sin dalle prime fasi, dato che sono fondamentali per l'avvio della transizione.

- **IAM**—AWS Identity and Access Management (IAM) costituisce la spina dorsale della distribuzione di AWS. Nel cloud devi creare un account e ottenere privilegi prima di poter eseguire il provisioning o l'orchestrazione delle risorse. Le storie tipiche sull'automazione possono riguardare la mappatura/concessione/audit di diritti, la gestione del materiale segreto, l'applicazione della separazione dei compiti e dell'accesso con privilegi minimi, la gestione just-in-time dei privilegi e la riduzione del ricorso a credenziali a lungo termine.
- **Logging e monitoraggio**—I servizi AWS forniscono una notevole quantità di dati di logging per aiutarti a monitorare le interazioni con la piattaforma. Le prestazioni dei servizi AWS basate sulle tue scelte di configurazione e la capacità di integrare log del sistema operativo e delle applicazioni per creare un quadro di riferimento comune. Le storie tipiche sull'automazione possono riguardare l'aggregazione dei log, soglie/allarmi/avvisi, l'arricchimento, la piattaforma di ricerca, la visualizzazione, l'accesso dei soggetti interessati e il flusso di lavoro e il ticketing per avviare la reazione closed-loop dell'organizzazione.
- **Sicurezza dell'infrastruttura**—Quando tratti l'infrastruttura come un codice, la sicurezza dell'infrastruttura diventa un carico di lavoro di primo

livello che deve essere distribuito anch'esso come codice. Questo approccio ti offre l'opportunità di configurare in modo programmatico i servizi AWS e di distribuire l'infrastruttura di sicurezza da AWS

I partner del marketplace, o soluzioni progettate autonomamente. Le storie tipiche sull'automazione possono riguardare la creazione di modelli personalizzati per configurare i servizi AWS in modo che soddisfino i tuoi requisiti, l'implementazione di modelli architetturali di sicurezza e i play di operazioni di sicurezza come codice, la progettazione di soluzioni di sicurezza personalizzate partendo dai servizi AWS, il ricorso a strategie di gestione delle patch come le distribuzioni blu/verdi, la riduzione della superficie esposta agli attacchi e la convalida dell'efficacia delle distribuzioni.

- **Protezione dei dati**—La tutela dei dati importanti è un elemento fondamentale della realizzazione e gestione dei sistemi di informazione e AWS fornisce servizi e caratteristiche che ti offrono opzioni solide per la protezione dei dati durante l'intero ciclo di vita. Le storie tipiche sull'automazione possono riguardare l'adozione di decisioni sulla collocazione dei carichi di lavoro, l'implementazione di uno schema di tagging, la costruzione di meccanismi per la protezione dei dati in movimento come connessioni VPN e TLS/SSL (incluso AWS Certificate Manager), la costruzione di meccanismi per la protezione dei dati inattivi attraverso la crittografia ai livelli idonei della tua infrastruttura, l'utilizzo dell'implementazione/integrazione di AWS Key Management Service (AWS KMS), la distribuzione di AWS CloudHSM, la creazione di schemi di tokenizzazione e l'implementazione e gestione di soluzioni AWS dei partner del marketplace.
- **Risposta agli eventi imprevisti**—L'automazione del processo di gestione degli eventi imprevisti migliora l'affidabilità e aumenta la velocità di risposta, creando spesso un ambiente più semplice da valutare nelle analisi che seguono l'azione. Le storie tipiche sull'automazione possono includere l'utilizzo della funzione "responders" di AWS Lambda che reagisce a modifiche specifiche dell'ambiente, l'orchestrazione di eventi di auto scaling, l'isolamento di componenti di sistema sospetti, la distribuzione just-in-time di strumenti investigativi e la creazione di flussi di lavoro e di ticket per concludere e imparare da una risposta organizzativa closed-loop.

Potenziamento degli elementi essenziali

Questi cinque Epics rappresentano i temi capaci di stimolare l'eccellenza operativa continua attraverso la disponibilità, l'automazione e l'audit. Si consiglia di integrare idoneamente questi Epics in ogni sprint. Quando occorre un'attenzione ulteriore, puoi valutare la possibilità di trattare tali aspetti come Epics a sé stanti.

- **Flessibilità**—Alta disponibilità, continuità delle operazioni, solidità e flessibilità e disaster recovery sono spesso altrettanti motivi per le distribuzioni cloud AWS. Le storie tipiche sull'automazione possono includere il ricorso a implementazioni Multi-AZ e Multi- Regione, la modifica della superficie di attacco disponibile, il dimensionamento e lo spostamento dell'allocazione delle risorse allo scopo di assorbire gli attacchi, salvaguardare le risorse esposte e indurre deliberatamente un malfunzionamento delle risorse per convalidare la continuità delle operazioni di sistema.

- **Convalida della compliance**—L'integrazione della compliance end-to-end nel programma di sicurezza evita che la compliance si riduca a un adempimento burocratico o a un elemento sovrapposto dopo la distribuzione. Questo Epic fornisce la piattaforma in grado di consolidare e razionalizzare gli artefatti di compliance generati con gli altri Epics. Le storie tipiche sull'automazione possono includere la creazione di test unitari di sicurezza per i requisiti di compliance, la progettazione di servizi e carichi di lavoro a supporto della raccolta di riscontri della compliance, la creazione di pipeline di notifica e visualizzazione per la compliance partendo da caratteristiche pensate per gli aspetti probatori, il monitoraggio continuo e la creazione di team DevSecOps orientati agli strumenti di compliance.

- **CI/CD sicuro (DevSecOps)**—La certezza della propria supply chain software maturata grazie all'uso di catene di strumenti di integrazione continua e distribuzione continua affidabili e convalidate è un modo mirato per far maturare prassi di gestione della sicurezza mentre si effettua la migrazione al cloud. Le storie tipiche sull'automazione possono includere la protezione avanzata e l'applicazione di patch alla catena di strumenti, l'accesso con privilegio minimo alla catena di strumenti, il logging e il monitoraggio del processo di produzione, l'integrazione della sicurezza/visualizzazione della distribuzione e il controllo dell'integrità del codice.

- **Configurazione e analisi di vulnerabilità**—La configurazione e l'analisi di vulnerabilità ottengono un notevole vantaggio dal dimensionamento, dall'agilità e dall'automazione consentiti da AWS. Le storie tipiche sull'automazione possono includere l'attivazione di AWS Config e la creazione di AWS Config Rules per i clienti, l'utilizzo di Amazon CloudWatch Events e di AWS Lambda per rispondere all'individuazione di modifiche, l'implementazione di Amazon Inspector, la scelta e la distribuzione di soluzioni di monitoraggio continuo da AWS Marketplace, la distribuzione di triggered scan e l'integrazione di strumenti di valutazione nella catena di strumenti CI/CD.
- **Big Data sulla sicurezza e analisi predittiva**—Le operazioni di sicurezza traggono vantaggio dai servizi e dalle soluzioni di Big Data al pari di qualunque altro aspetto di business. Lo sfruttamento dei Big Data fornisce informazioni ancora più approfondite in modo più tempestivo, rafforzando in tal modo l'agilità e la capacità di eseguire iterazioni su larga scala nell'assetto di sicurezza. Le storie tipiche sull'automazione possono includere la creazione di data lake di sicurezza, lo sviluppo di pipeline di analisi, la creazione della visualizzazione per favorire il decision making in materia di sicurezza e la creazione di meccanismi di feedback per la risposta autonoma.

Dopo la definizione di tale struttura, è possibile creare un piano di implementazione. Le funzionalità cambiano nel tempo e vengono continuamente identificate opportunità di miglioramento. Nota: i temi o le categorie di funzionalità illustrate sopra possono essere trattati come Epics nel quadro di una metodologia che contenga una gamma di user story comprensive sia di casi d'uso sia di casi d'abuso. Più sprint portano a una maggiore maturità, senza perdere, allo stesso tempo, la flessibilità di adattarsi al ritmo e alla domanda del business.

Esempio di Serie di sprint

Valuta la possibilità di organizzare un set campione di sei sprint di due settimane (un gruppo di Epics spalmato su un trimestre civile di dodici settimane), compreso un breve periodo preparatorio, come segue. L'approccio adottato dipenderà dalla disponibilità di risorse, dalla priorità e dal livello di maturità desiderato in ciascuna capacità, mentre si procede verso la capacità produttiva minima funzionante (MVP).

- **Sprint 0**—Cartografia della sicurezza: mappatura della compliance, mappatura delle policy, revisione del threat model iniziale, creazione del registro dei rischi; realizzazione di un portafoglio di casi d'uso e d'abuso; pianificazione dei Security Epics
- **Sprint 1**—IAM; logging e monitoraggio
- **Sprint 2**—IAM; logging e monitoraggio; protezione dell'infrastruttura
- **Sprint 3**—IAM; logging e monitoraggio; protezione dell'infrastruttura
- **Sprint 4**—IAM; logging e monitoraggio; protezione dell'infrastruttura; protezione dei dati
- **Sprint 5**—Protezione dei dati, automazione delle operazioni di sicurezza, pianificazione/strumenti per la risposta agli eventi imprevisti; flessibilità
- **Sprint 6**—Automazione delle operazioni di sicurezza; risposta agli eventi imprevisti; flessibilità

Un elemento essenziale della convalida della compliance è l'integrazione della convalida in ciascuno sprint attraverso singoli test case della sicurezza e della compliance e successivamente il passaggio al processo di produzione. Quando occorre una capacità esplicita di convalida della compliance, possono essere stabiliti sprint orientati specificamente a tali user story. Con il tempo, è possibile utilizzare l'iterazione per conseguire la convalida continua e l'implementazione dell'autocorrezione dello scostamento, ove opportuno.

L'approccio globale intende definire chiaramente cosa sia un MVP o una baseline, per mapparli successivamente al primo sprint in ciascuna area. Nelle prime fasi l'obiettivo finale può essere meno definito, ma viene creata una roadmap chiara degli sprint iniziali. La tempistica, l'esperienza e l'iterazione permetteranno di affinare e adeguare lo stato finale affinché sia perfettamente adatto all'organizzazione. Nella realtà, lo stato finale può cambiare costantemente, ma alla fine il processo porta comunque al miglioramento continuo ad un ritmo più

rapido. Questo approccio può essere più efficace e maggiormente conveniente rispetto a un approccio "big bang", basato su tempistiche lunghe e su elevati esborsi di capitale.

Volendo scendere un po' più nel dettaglio, il primo sprint per IAM può consistere nella definizione della struttura degli account e nell'implementazione dell'insieme principale di best practice. Un secondo sprint può implementare la federazione. Un terzo sprint può espandere la gestione degli account per rispondere alle esigenze di più account e via dicendo. Le user story relative a IAM che riguardino uno o più di questi sprint iniziali potrebbero includere storie come queste:

"In quanto amministratore degli accessi, voglio creare un primo gruppo di utenti per la gestione delle relazioni di trust dei provider dell'accesso privilegiato e dell'identità federata".

"In quanto amministratore degli accessi, voglio mappare gli utenti presenti nella directory aziendale esistente a ruoli funzionali o a set di diritti di accesso, sulla piattaforma AWS".

"In quanto amministratore degli accessi, voglio utilizzare l'autenticazione multi-factor su qualsiasi interazione con la console AWS da parte di utenti interattivi".

In questo esempio, le seguenti user story su logging e monitoraggio possono riguardare uno o più sprint iniziali:

"In quanto analista delle operazioni di sicurezza, voglio ricevere log a livello di piattaforma per tutte le regioni AWS e gli account AWS".

"In quanto analista delle operazioni di sicurezza, voglio che tutti i log a livello di piattaforma siano distribuiti a un'ubicazione condivisa da tutte le regioni AWS e gli account".

"In quanto analista delle operazioni di sicurezza, voglio ricevere avvisi riguardo a qualsiasi operazione che colleghi policy IAM a utenti, gruppi o ruoli".

È possibile creare capacità in parallelo o in serie e mantenere la flessibilità includendo user story sulle capacità di sicurezza nel portafoglio globale dei prodotti. È anche possibile dividere le user story in un team DevOps incentrato sulla sicurezza. Si tratta di decisioni che è possibile rivedere periodicamente, in modo da definire una distribuzione su misura in base alle esigenze dell'organizzazione nel tempo.

Considerazioni

- **Riesamina** il framework di controllo esistente per stabilire in che modo i servizi AWS saranno gestiti per soddisfare gli standard di sicurezza richiesti.
- **Definisci** i soggetti e poi crea lo storyboard della loro esperienza di interazione con i servizi AWS.
- **Definisci** che cos'è il primo sprint e quale sarà l'obiettivo iniziale di alto livello e di più lungo periodo.
- **Definisci** una baseline di sicurezza minima realizzabile ed effettua iterazioni continue per aumentare le aspettative riguardo ai carichi di lavoro e ai dati che stai proteggendo.

Il viaggio da compiere – Sviluppo di operazioni di sicurezza efficaci

In un ambiente in cui l'infrastruttura è un codice, anche la sicurezza deve essere trattata come un codice. Il componente delle operazioni di sicurezza fornisce gli strumenti per comunicare e rendere operativi i principi fondamentali della sicurezza come codice:

- Usa il cloud per proteggere il cloud.
- L'infrastruttura di sicurezza dovrebbe essere compatibile con il cloud.
- Esponi le caratteristiche di sicurezza come servizi con l'ausilio dell'API.
- Automatizza ogni aspetto, affinché la sicurezza e la compliance possano essere ricalibrate.

Per rendere realizzabile questo modello di governance, spesso le line of business si organizzano sotto forma di team DevOps per realizzare e distribuire il software per l'infrastruttura e il business. È possibile estendere i principi fondamentali del modello di governance attraverso l'integrazione della sicurezza nella cultura o nelle prassi DevOps, un processo che viene talvolta denominato DevSecOps. Crea un team sulla base dei seguenti principi:

- Il team di sicurezza unisce culture e comportamenti DevOps.
- Gli sviluppatori contribuiscono apertamente al codice utilizzato per automatizzare le operazioni di sicurezza.
- Il team delle operazioni di sicurezza può partecipare al test e all'automazione del codice dell'applicazione.
- Il team considera un vanto la rapidità e la frequenza delle sue distribuzioni. La distribuzione più frequente, con modifiche più piccole, riduce il rischio operativo ed evidenza progressi rapidi rispetto alla strategia di sicurezza.

I team integrati dello sviluppo, della sicurezza e delle operazioni hanno tre mission fondamentali condivise:

- Proteggere la catena di strumenti dell'integrazione continua/distribuzione continua.
- Consentire e promuovere lo sviluppo di software flessibile mentre attraversa la catena di strumenti.

- Distribuire tutta l'infrastruttura e il software di sicurezza tramite la catena di strumenti.

Stabilire le (eventuali) modifiche alle prassi di sicurezza attuali aiuterà a pianificare una strategia corretta di adozione di AWS.

Conclusioni

Nel momento in cui stai iniziando il viaggio verso l'adozione di AWS, forse vorrai aggiornare il tuo assetto di sicurezza per includere la porzione AWS nel tuo ambiente. Questo whitepaper sulla prospettiva di sicurezza fornisce indicazioni prescrittive su un approccio in grado di sfruttare i vantaggi per l'assetto di sicurezza offerti dall'utilizzo di AWS. Molte altre informazioni sulla sicurezza sono disponibili nel sito Web di AWS, dove le caratteristiche di sicurezza sono descritte in modo dettagliato e sono fornite ulteriori indicazioni prescrittive dettagliate per le implementazioni comuni. È inoltre disponibile un elenco completo di contenuti relativi alla sicurezza[4] che dovrebbero essere consultati da vari membri del team di sicurezza durante la preparazione alle iniziative per l'adozione di AWS.

Appendice A: Monitoraggio dei progressi nella prospettiva di sicurezza AWS CAF

Puoi utilizzare i principali fattori di sicurezza e il modello dei progressi dei Security Epics esaminati in questa appendice per misurare i progressi e la maturità dell'implementazione della prospettiva di sicurezza AWS CAF. Tali fattori e il modello dei progressi possono essere utilizzati per la pianificazione dei progetti, per valutare l'efficacia delle implementazioni o semplicemente come mezzo per stimolare la conversazione sui passi futuri.

Principali fattori per la sicurezza

I principali fattori per la sicurezza sono milestone che aiutano a tenere fede agli obiettivi. Utilizziamo un modello a punteggio costituito da tre valori: Irrisolto, Attivato e Completato.

- Strategia di sicurezza nel cloud [Irrisolto, Attivato, Completato]
- Piano di comunicazione agli stakeholder [Irrisolto, Attivato, Completato]
- Cartografia della sicurezza [Irrisolto, Attivato, Completato]
- Modello di responsabilità condivisa dei documenti [Irrisolto, Attivato, Completato]
- Playbook e runbook delle operazioni di sicurezza [Irrisolto, Attivato, Completato]
- Piano dei Security Epics [Irrisolto, Attivato, Completato]
- Simulazione della risposta a un evento imprevisto di sicurezza [Irrisolto, Attivato, Completato]

Modelli dei progressi nei Security Epics

Il modello dei progressi nei Security Epics aiuta a valutare i progressi nell'implementazione dei 10 Security Epics descritti in questo whitepaper. Utilizziamo un modello di punteggio da 0 (zero) a 3 per misurare l'efficacia. Abbiamo fornito esempi per i Security Epics di Identity and Access Management e Logging e monitoraggio, per consentirti di comprendere facilmente come funziona questa progressione.

5 principali Security Epics 0-Irrisolto

1- Risolto nell'architettura e nei piani

2- Implementazione minima realizzabile

3- Implementazione della produzione pronta per l'impresa

Security Epic	0	1	2	3
Identity and Access Management	Esempio: Nessuna relazione tra identità in locale e AWS.	Esempio: Viene definito un approccio per la gestione delle identità del ciclo di vita della forza lavoro. L'architettura IAM è documentata. Le funzioni lavorative sono mappate alle esigenze delle policy IAM.	Esempio: IAM implementata come definita nell'architettura. Implementate policy IAM che sono mappate ad alcune funzioni lavorative. Convalidata l'implementazione IAM.	Esempio: Automazione dei flussi di lavoro del ciclo di vita IAM.
Logging e monitoraggio	Esempio: Nessun utilizzo delle soluzioni di logging e monitoraggio fornite da AWS.	Esempio: Viene definito un approccio per l'aggregazione dei log, il monitoraggio e l'integrazione nei processi di gestione degli eventi di sicurezza.	Esempio: Il logging a livello di piattaforma e a livello di servizio è attivato e centralizzato.	Esempio: Gli eventi con implicazioni per la sicurezza sono profondamente integrati nel flusso di lavoro della sicurezza e nei processi e sistemi per la gestione degli eventi imprevisti.
Sicurezza dell'infrastruttura				
Protezione dei dati				
Gestione degli eventi imprevisti				

Potenziamento dei 5 elementi essenziali 0- Irrisolto

1- Risolto nell'architettura e nei piani

2- Implementazione minima realizzabile

3- Implementazione della produzione pronta per l'impresa

Security Epic	0	1	2	3
Flessibilità				
DevSecOps				
Convalida della compliance				
Configurazione e gestione di vulnerabilità				
Big Data sulla sicurezza				

Tassonomia e termini CAF

Il framework per l'adozione del cloud (Cloud Adoption Framework, CAF) è un framework AWS creato per acquisire linee guida e best practice da precedenti engagement dei clienti. Una *prospettiva* AWS CAF rappresenta un'area di interesse pertinente ai fini dell'implementazione di sistemi IT basati su cloud nelle organizzazioni. Ad esempio, la Prospettiva di sicurezza fornisce linee guida e processi per valutare e migliorare i controlli di sicurezza esistenti mentre si effettua la transizione a un ambiente AWS.

Ogni Prospettiva CAF è costituita da componenti e attività. Un *componente* è una sotto-area di una prospettiva che rappresenta un aspetto specifico che merita attenzione.
Il presente whitepaper illustra i componenti della Prospettiva di sicurezza.
Un'*attività* fornisce linee guida maggiormente prescrittive per la creazione di piani realizzabili che l'organizzazione può utilizzare per passare al cloud e gestire soluzioni basate su cloud in maniera continuativa.

Ad esempio, il componente di *Indicazione* è uno dei componenti della Prospettiva d sicurezza e la definizione di un modello di responsabilità condivisa AWS su misura per il tuo ecosistema può essere un'attività all'interno di tale componente.

Quando sono combinati, Cloud Adoption Framework (CAF) e Cloud Adoption Methodology (CAM) possono essere utilizzati come linee guida durante la transizione verso il cloud AWS.

Note

1 https://d0.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf

2 https://aws.amazon.com/compliance/

3 https://aws.amazon.com/compliance/shared-responsibility-model/

4 https://aws.amazon.com/security/security-resources/