Incrementa la sicurezza del cloud ibrido

Proteggi la tua azienda grazie ad alcune considerazioni chiave sulla sicurezza cloud native

/Considera tutte le possibilità

Red Hat

Di Lucy Huh Kerner, Director, Security Global Strategy and Evangelism, Red Hat

Contenuti

Capitolo 1

Adotta un cloud ibrido incentrato sulla sicurezza

L'adozione del cloud è in forte aumento. Infatti, il 65% delle organizzazioni afferma di fare largo uso di soluzioni cloud e il 72% delle aziende dichiara di avere in atto una strategia di cloud ibrido.[1]

Il cloud ibrido è un modello architetturale che offre un discreto livello di portabilità, di orchestrazione e di gestione dei carichi di lavoro su due o più ambienti connessi ma separati, inclusi ambienti bare metal, virtualizzati, cloud privati e pubblici. Con un'architettura di cloud ibrido è possibile eseguire i carichi di lavoro in qualsiasi ambiente connesso, trasferendo e utilizzando le risorse tra i diversi ambienti.

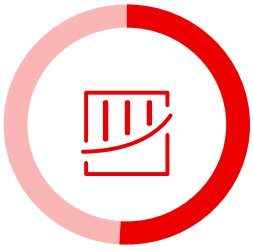
L'adozione di ambienti cloud ibridi garantisce alle organizzazioni i seguenti vantaggi:

- Fruibilità di infrastrutture, piattaforme, applicazioni e strumenti di diversi fornitori grazie a una completa interconnessione.
- Efficienza e scalabilità maggiori.
- Riduzione dei costi.
- Agilità migliorata.
- Posizionamento dei dati ottimizzato.

[1] Flexera, "Flexera 2023 State of the Cloud Report", marzo 2023.

A prescindere dal grado di transizione al cloud ibrido raggiunto, la sicurezza è una delle preoccupazioni principali, con il 79% delle aziende che la vede come una vera e propria sfida.[1] Le vulnerabilità nella sicurezza del cloud ibrido sono spesso legate a: controllo sulle risorse insufficiente o inefficace (incluso l'utilizzo di cloud pubblico non approvato), mancanza di visibilità sulle risorse, controllo delle modifiche inadeguato, gestione della configurazione carente, controlli degli accessi non efficaci, errore umano, ecc. Gli utenti non autorizzati possono sfruttare a proprio vantaggio queste lacune per accedere a dati sensibili e risorse interne, con ripercussioni economiche anche importanti sull'azienda.

A livello mondiale il costo medio di una violazione dei dati ha raggiunto un nuovo record nel 2023 toccando i **US$ 4,45 milioni**, con una perdita di opportunità commerciali pari al **29,2%** di tale cifra.[2]



51%

delle aziende che ha subito una violazione dei dati progetta di aumentare gli investimenti sulla sicurezza.[2]

[1] Flexera, "Flexera 2023 State of the Cloud Report", marzo 2023.
[2] IBM Security, "Cost of a Data Breach Report 2023", 2023.

Nel 2023 sono aumentati sia il costo medio per record coinvolto in una violazione dei dati sia il tempo necessario per contenere le violazioni.[2] Adattando le proprie metodologie perché tengano conto delle differenze tra le architetture cloud e on premise, è possibile distribuire un cloud ibrido incentrato sulla sicurezza e far fronte alle sfide moderne. Questo ebook illustra alcuni approcci innovativi e offre utili spunti di riflessione per la sicurezza del cloud ibrido.

277 giorni

Tempo medio necessario per identificare e contenere una violazione dei dati nel 2023.[2]

US$ 1,02 milioni

Risparmio sui costi ottenibile riuscendo a identificare e contenere una violazione entro 200 giorni.[2]

[2] IBM Security, "Cost of a Data Breach Report 2023", 2023.

Capitolo 2

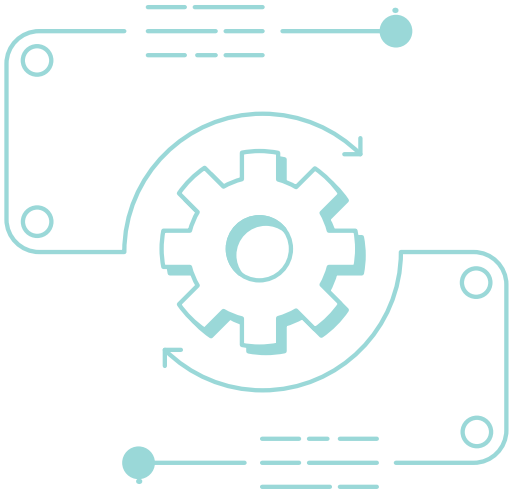
La sicurezza è un processo in continua evoluzione

Per ottenere una sicurezza efficace serve un approccio olistico che tenga in considerazione persone, processi e tecnologie. Eseguire il deployment di prodotti e strumenti incentrati sulla sicurezza non basta a proteggere l'infrastruttura, il cloud o l'azienda. Occorre definire strategie e processi di sicurezza che consentano di sfruttare al meglio le funzionalità dei prodotti e ridurre i rischi.

Tali strategie e processi dovranno poi essere adattati nel tempo in base all'evoluzione di tecnologie, minacce e necessità aziendali. Negli ambienti cloud ibridi, che non presentano confini definiti, gli approcci tradizionali sono inefficaci e occorre gestire la sicurezza in maniera completamente nuova.

La gestione centralizzata delle identità e il controllo degli accessi sono elementi fondamentali per gli approcci alla sicurezza basati sul cloud, in quanto entrambi sfruttano il principio dei privilegi minimi per fornire agli utenti l'accesso solo a ciò di cui hanno effettivamente bisogno. Questo approccio prevede di svolgere un controllo iniziale per determinare i diritti di accesso di cui dispone ogni utente e una successiva rivalutazione per stabilire il livello di accesso più idoneo per ciascuno.

Inoltre, una strategia efficace per la sicurezza del cloud ibrido deve essere caratterizzata da misure di difesa avanzate e multilivello che consentano di utilizzare le funzionalità di tutto l'ambiente, inclusi sistemi operativi, piattaforme per container e strumenti di automazione.



Sistema operativo

Adotta strumenti integrati in grado di aiutarti a garantire la conformità ai requisiti di sicurezza, implementare misure protettive fisiche, migliorare la sicurezza della rete, controllare gli accessi degli utenti, isolare i processi e incrementare la sicurezza dei dati. Tra questi ricordiamo OpenSCAP, USBGuard, Security-Enhanced Linux® (SELinux), gestione delle identità e Network Bound Disk Encryption.

Piattaforma per container

Utilizza funzionalità integrate all'interno della piattaforma e di Kubernetes per migliorare la sicurezza dei container. Tra queste sono inclusi i criteri di sicurezza del pod, i controlli del traffico di rete, i controlli di cluster in entrata e in uscita, i controlli degli accessi basati sui ruoli (RBAC), la gestione integrata dei certificati e la microsegmentazione della rete.

Strumenti di automazione

Scegli una piattaforma e un linguaggio di automazione intuitivi cosicché ogni membro dell'organizzazione, inclusi i team di sviluppo, operativi, di sicurezza e di conformità, possano impararne il funzionamento e utilizzarli. Implementa funzionalità di controllo degli accessi, logging e verifica.

È essenziale rivedere anche i processi e gli strumenti di sicurezza già in uso. Assicurati di utilizzare tutte le funzionalità disponibili e stabilisci se alcune impostazioni possano essere modificate o riconfigurate per fornire una protezione migliore o se siano necessari nuovi processi e strumenti.

1. Crea un inventario delle risorse IT e degli strumenti in uso.
2. Verifica le architetture di sicurezza e di rete, i criteri di sicurezza informatica e i processi di lavoro esistenti e stabilisci eventuali lacune nelle competenze.
3. Definisci un modello delle minacce, determinando la tolleranza al rischio, e le strategie per la riduzione delle violazioni alla sicurezza informatica.
4. Analizza le architetture, i criteri e i processi per identificare le aree da migliorare.
5. Valuta gli strumenti e le risorse in uso per capire se sono in grado di supportare le nuove strategie e i nuovi processi. Pianifica come gestire qualsiasi eventuale lacuna nella sicurezza.

I prossimi capitoli illustrano alcune considerazioni chiave sulla sicurezza del cloud ibrido e offrono validi consigli per migliorare la protezione degli ambienti IT.

Capitolo 3

Considerazione sulla sicurezza n. 1

Adotta una base solida

Perché è importante?

Quando si distribuiscono i carichi di lavoro in più ambienti o si utilizzano tecnologie open source non verificate, individuare le vulnerabilità diventa molto complicato. Inoltre, senza una base di sicurezza solida è pressoché impossibile adottare una strategia di sicurezza multilivello efficace che consenta di ridurre i rischi. L'utilizzo di software open source distribuiti direttamente dalle community upstream può esporre a potenziali rischi di sicurezza e attacchi alla catena di distribuzione, in cui gli hacker approfittano di punti deboli nei servizi e nei software di terze parti per raggiungere il loro obiettivo finale. Gli attacchi alla sicurezza sono di varie tipologie e possono includere hijack degli aggiornamenti software o inserimento di un codice dannoso in programmi software legittimi. Negli ultimi tre anni gli attacchi alla catena di distribuzione del software sono aumentati in media del 742% su base annua.[3] Ecco perché predisporre una base unificata, stabile e incentrata sulla sicurezza è fondamentale per proteggere le aziende.

Consigli e best practice

Riduci i rischi per la sicurezza della catena di distribuzione del software scegliendo una soluzione open source di livello enterprise offerta da un fornitore affidabile come Red Hat che garantisce il supporto per l'intero ciclo di vita del software. I fornitori di soluzioni open source di livello enterprise sviluppano i loro prodotti seguendo un solido processo per la sicurezza della catena di distribuzione del software, che comprende la selezione dei software open source per conto dei loro clienti. In questo modo i clienti sono sicuri di utilizzare soluzioni open source affidabili, resilienti e comprovate.

Inoltre, è fondamentale eseguire le applicazioni principali su una piattaforma con funzionalità di sicurezza integrate. Questo garantisce un livello di sicurezza di base da cui i clienti possono partire per eseguire le applicazioni critiche, introdurre funzionalità di sicurezza multilivello per ridurre i rischi e automatizzare la sicurezza e la conformità.

Metti al primo posto la sicurezza di applicazioni e processi optando per un sistema operativo affidabile e resiliente che fornisce stabilità e sicurezza avanzate come Red Hat® Enterprise Linux®. Questa soluzione offre una base solida per la scalabilità affidabile delle applicazioni principali, la conformità ai requisiti di sicurezza e l'adozione coerente di tecnologie emergenti in ambienti bare metal, virtuali, containerizzati e in tutti i tipi di cloud.

[3] Sonatype, "9th Annual State of the Software Supply Chain", 2023.

Red Hat Enterprise Linux, che è la base di numerose soluzioni Red Hat, è un sistema operativo affidabile scelto da molte aziende proprio per le sue funzionalità di sicurezza integrate.

Red Hat Enterprise Linux consente di:

Tutelare i dati e i sistemi grazie a funzionalità di sicurezza integrate come l'applicazione live delle patch al kernel, ovvero l'applicazione delle patch di sicurezza senza bisogno di riavviare o interrompere i sistemi. Tra le altre funzionalità di sicurezza integrate ricordiamo gli elenchi di applicazioni consentite con cui è possibile specificare le applicazioni e i file approvati che un certo utente è autorizzato a eseguire in un sistema; e SELinux per controllare in maniera puntuale file, processi, utenti e applicazioni.

Automatizzare la protezione dei dati in maniera scalabile e garantirne la sicurezza nel tempo grazie a funzionalità di sicurezza integrate come la tecnologia Network Bound Disk Encryption, che permette di automatizzare lo sblocco dei sistemi crittografati senza gestire manualmente le chiavi crittografiche. Inoltre, l'adozione di criteri di crittografia a livello di sistema aiuta a semplificare la sicurezza dei dati e la conformità grazie a parametri di crittografia coerenti e personalizzabili per rispondere ai requisiti specifici del sito.

Soddisfare i requisiti di conformità e semplificare gli audit. Red Hat Enterprise Linux integra funzionalità di verifica e correzione della conformità (OpenSCAP) con cui è possibile analizzare la configurazione e le vulnerabilità di un sistema locale per convalidarne la conformità a diversi standard di sicurezza del settore.

Tutti i prodotti Red Hat che vengono eseguiti su Red Hat Enterprise Linux beneficiano del suo approccio alla sicurezza, come ad esempio **Red Hat OpenShift** che offre protezione avanzata per container e Kubernetes. Le funzionalità di sicurezza di Red Hat si estendono all'intero stack, inclusi i componenti Kubernetes. Allo stesso modo anche **Red Hat Ansible Automation Platform** offre funzionalità di sicurezza integrate con cui le aziende possono automatizzare la sicurezza e la conformità in maniera scalabile.

Azioni strategiche

Segui questi suggerimenti per favorire la sicurezza del cloud ibrido:

Passa alle versioni commerciali

Esegui la migrazione dai software open source distribuiti direttamente dalle community upstream alle versioni commerciali più affidabili. Le versioni commerciali vengono testate e convalidate per ridurre il rischio di bug e vulnerabilità nella sicurezza. Includono in genere anche il supporto di livello enterprise, un servizio che permette di ottenere le patch di sicurezza rapidamente e assiste i clienti nella configurazione del software per garantire risultati ottimali. Puntando su software open source di livello enterprise offerti da un fornitore affidabile, avrai la certezza di adottare prodotti sviluppati seguendo un solido processo per la sicurezza della catena di distribuzione del software e disporrai del supporto per l'intero ciclo di vita del software. È un ottimo modo per continuare a beneficiare dell'innovazione open source in tutta sicurezza.

Scegli una piattaforma con funzionalità di sicurezza integrate

È fondamentale scegliere delle piattaforme (sistema operativo, piattaforma applicativa containerizzata e piattaforma di automazione) con funzionalità di sicurezza integrate. Questo garantisce un livello di sicurezza di base da cui i clienti possono partire per eseguire le applicazioni critiche, introdurre funzionalità di sicurezza multilivello per ridurre i rischi e automatizzare la sicurezza e la conformità in maniera scalabile.

Estendi la sicurezza all'intero stack tecnologico

Dopo aver poggiato le basi della sicurezza, assicurati che le tecnologie che verranno eseguite sulle piattaforme sottostanti beneficino delle stesse funzionalità di sicurezza e operino in sinergia in modo da ottenere una sicurezza multilivello.

Capitolo 4

Considerazione sulla sicurezza n. 2

Migliora l'affidabilità della catena di distribuzione del software con DevSecOps

Perché è importante?

Nel 2023 il 12% delle violazioni dei dati è nato da un attacco alla catena di distribuzione del software.[2] L'utilizzo di software open source non verificati e distribuiti direttamente dalle community upstream può causare vulnerabilità nella sicurezza ed esporre ad attacchi alla catena di distribuzione, in cui gli hacker approfittano di punti deboli nei servizi e nei software di terze parti per raggiungere il loro obiettivo finale. Gli attacchi alla sicurezza sono di varie tipologie e possono includere hijack degli aggiornamenti software o inserimento di un codice dannoso in programmi software legittimi.

Gli approcci alla sicurezza compartimentalizzati causano spesso lacune nella sicurezza e un utilizzo inefficiente delle risorse: questo perché la sicurezza non viene integrata fin dall'inizio nel processo di sviluppo applicativo e di deployment dell'infrastruttura, ma rimane un aspetto secondario. Considerando però la ricerca di cicli di sviluppo sempre più rapidi e modelli di deployment sempre più flessibili, riuscire a integrare la sicurezza lungo tutto il processo è quanto mai importante.

Consigli e best practice

Per adottare un approccio incentrato sulla sicurezza della catena di distribuzione del software, occorre innanzitutto coltivare una mentalità DevSecOps. Questo tipo di mentalità punta a favorire la collaborazione tra sviluppatori di applicazioni, team operativi IT e team di sicurezza al fine di implementare la sicurezza della catena di distribuzione del software lungo tutto il ciclo di vita dello sviluppo del software (SDLC) e il ciclo di vita dell'infrastruttura; il tutto operando su una base open source di livello enterprise in ambiente cloud ibrido.

[2] IBM Security, "Cost of a Data Breach Report 2023", 2023.

DevSecOps automatizza l'integrazione della sicurezza in tutte le fasi del ciclo di vita dello sviluppo del software, dalla progettazione, all'integrazione, al test, al deployment, alla distribuzione.

La metodologia DevSecOps offre i seguenti vantaggi:

- Aiuta i team IT e di sicurezza a gestire le difficoltà che coinvolgono persone, processi e tecnologie.
- Migliora l'efficienza, la coerenza, la ripetibilità e la collaborazione.
- Limita l'errore umano e quindi riduce i rischi.

Con DevSecOps la sicurezza diventa una responsabilità condivisa ed è integrata dall'inizio alla fine. Invece di delegare la definizione dei criteri di sicurezza a un unico team isolato, si hanno sviluppatori, team operativi e di sicurezza che lavorano fianco a fianco condividendo visibilità e feedback, e mettendo a frutto le nozioni apprese e le informazioni importanti acquisite. Questo approccio aumenta la protezione dell'intero stack IT poiché prevede che la sicurezza sia parte integrante dello sviluppo applicativo e del deployment dell'infrastruttura sin dal principio.

Gli sviluppatori di applicazioni aziendali che creano nuove funzionalità software per le proprie organizzazioni hanno bisogno di aumentare i livelli di sicurezza e ridurre il carico cognitivo. La sicurezza deve essere implementata in tutto l'SDLC: in fase di codifica attraverso controlli integrati alla sicurezza dell'applicazione per individuare tempestivamente eventuali problemi nell'SDLC e ridurre i tempi di fermo prolungati; in fase di creazione grazie all'utilizzo di flussi di lavoro di integrazione e distribuzione continue (CI/CD) incentrati sulla sicurezza per proteggere i sistemi di compilazione; e in fase di distribuzione ed esecuzione con golden path, analisi delle vulnerabilità, firme degli artefatti, attestazioni, provenienza, punti di applicazione dei criteri e distinte base del software (SBOM).

Occorre inoltre che la propria strategia garantisca: l'affidabilità delle fonti da cui provengono le tecnologie open source, l'adozione di flussi di automazione continua per l'applicazione di patch e aggiornamenti e l'integrazione della sicurezza in tutti i processi e componenti del progetto. Ed è fondamentale incoraggiare l'utilizzo di soluzioni open source di livello enterprise che includano un supporto adatto a contesti aziendali per l'intero ciclo di vita.

Adottando le soluzioni open source di livello enterprise offerte da Red Hat, le aziende possono beneficiare dell'esperienza trentennale matura dall'azienda nell'ambito della sicurezza della catena di distribuzione del software open source. La gamma di prodotti Red Hat permette di distribuire, gestire e garantire la sicurezza dei cluster Kubernetes e offre piattaforme unificate per snellire lo sviluppo, la modernizzazione, il deployment e la scalabilità delle applicazioni.

Red Hat OpenShift Platform Plus è una piattaforma unificata che include Red Hat OpenShift, Red Hat Advanced Cluster Security for Kubernetes, Red Hat Advanced Cluster Management for Kubernetes, Red Hat Quay e Red Hat OpenShift Data Foundation. Si tratta di una soluzione ideale per lo sviluppo, la modernizzazione, il deployment e la scalabilità delle applicazioni containerizzate in Kubernetes. Prevede la sicurezza degli ambienti multicluster e la gestione di conformità, dati e applicazioni per assicurare una catena di distribuzione del software coerente dall'inizio alla fine.

Azioni strategiche

Segui questi suggerimenti per implementare DevSecOps e migliorare la sicurezza della catena di distribuzione del software:

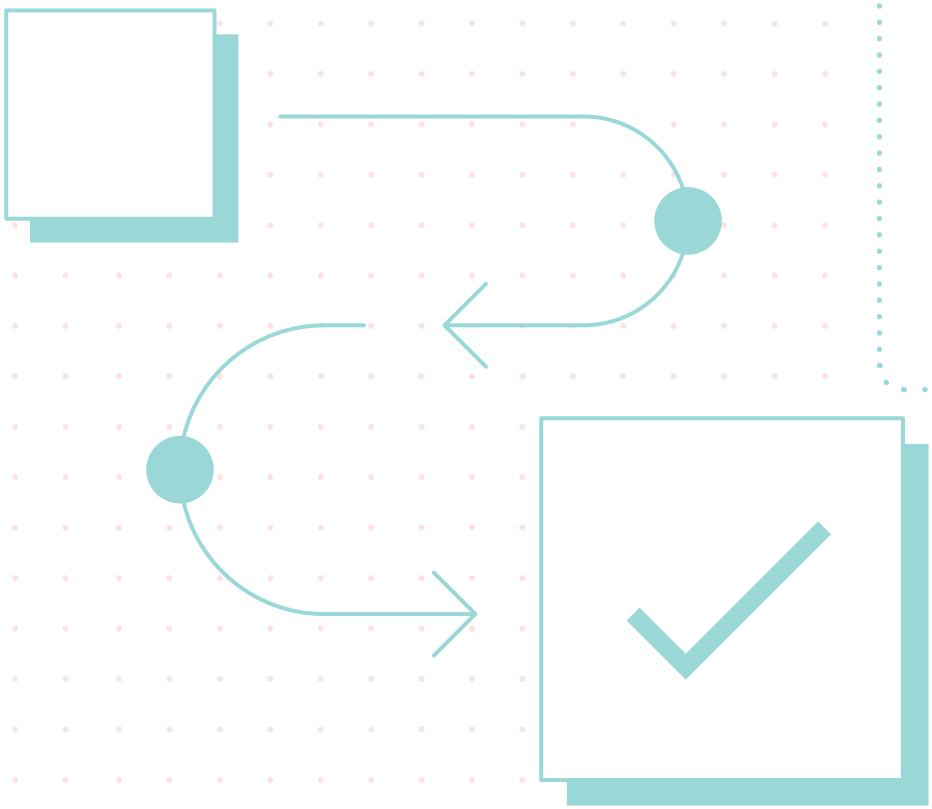
Adotta un approccio graduale.
Inizia in piccolo selezionando un solo progetto. Incoraggia la sperimentazione e il miglioramento continuo e iterativo per perfezionare e ottimizzare i processi. Condividi i progetti di successo mostrandone il valore al resto dell'organizzazione.

Definisci tempistiche e obiettivi condivisi e chiari.
La trasparenza è essenziale. Assicurati che tutte le persone coinvolte comprendano e condividano gli obiettivi e le tempistiche del progetto.

Forma il personale in diverse aree.
Definisci percorsi formativi sulla sicurezza, sull'infrastruttura e sullo sviluppo che siano regolarmente aggiornati e sempre accessibili da tutti i membri del team.

Crea un gruppo di lavoro sulla sicurezza.
Metti insieme un team integrato e interdisciplinare che definisca degli scenari di utilizzo e le strategie in ambito di sicurezza. Amplia le conoscenze grazie al confronto diretto tra esperti e sfrutta i risultati delle ricerche delle altre organizzazioni.

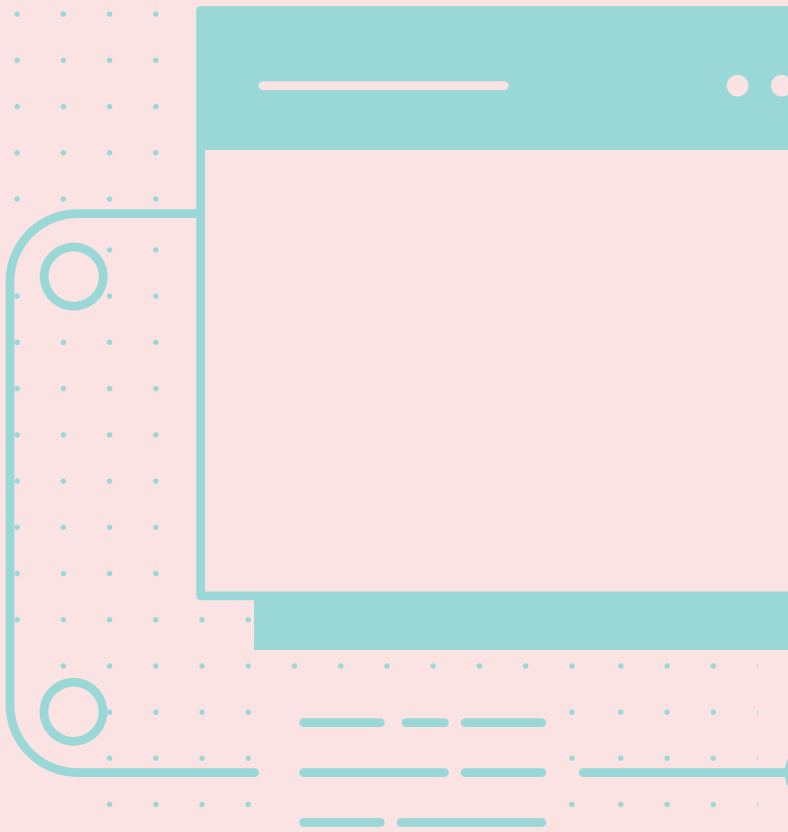
Implementa la sicurezza in tutto l'SDLC con una piattaforma applicativa unificata.
La sicurezza deve essere implementata in tutto l'SDLC: in fase di codifica attraverso controlli integrati alla sicurezza dell'applicazione per individuare tempestivamente eventuali problemi nell'SDLC e ridurre i tempi di fermo prolungati; in fase di creazione grazie all'utilizzo di flussi di lavoro di integrazione e distribuzione continue (CI/CD) incentrati sulla sicurezza per proteggere i sistemi di compilazione; e in fase di distribuzione ed esecuzione con golden path, analisi delle vulnerabilità, firme degli artefatti, attestazioni, provenienza, punti di applicazione dei criteri e distinte base del software (SBOM).



Capitolo 5

Considerazione sulla sicurezza n. 3

Utilizza automazione e gestione per proteggere il cloud ibrido



Perché è importante?

Gli errori di configurazione e un controllo delle modifiche inadeguato sono le minacce principali alla sicurezza,[4] perché rendono i sistemi vulnerabili agli attacchi. Il controllo delle modifiche è fondamentale per sapere chi ha modificato le configurazioni, e quando e quali modifiche ha apportato nell'ambito dei cicli di vita del sistema.

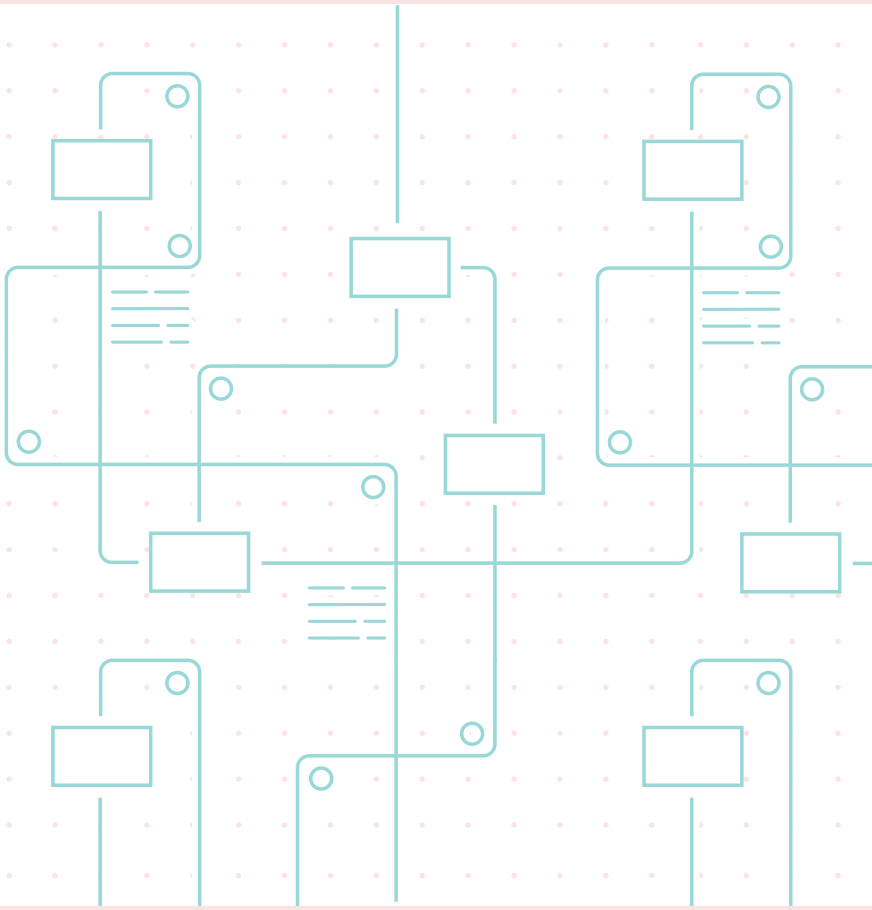
L'automazione, la gestione e l'intelligenza artificiale (IA) consentono di semplificare le operazioni quotidiane e integrare la sicurezza nei processi, nelle applicazioni e nell'infrastruttura fin dal principio. Disporre di una strategia di gestione e automazione estesa all'intera azienda aiuta a ridurre l'errore umano e migliora la velocità, la coerenza, la ripetibilità, oltre a permettere la verifica e gli audit. Una strategia di gestione e automazione centralizzata incrementa la sicurezza e la conformità perché semplifica l'implementazione di un modello DevSecOps, che prevede l'integrazione della sicurezza fin dalle prime fasi dello sviluppo applicativo e delle operazioni IT e per tutto il ciclo di vita. In effetti, l'utilizzo massiccio di automazione, gestione e IA nei processi di sicurezza riduce il costo medio di una violazione dei dati del 39,3%. Purtroppo però solo il 28% delle organizzazioni sfrutta questa incredibile opportunità.[2]

[2] IBM Security, "Cost of a Data Breach Report 2023", 2023.

[4] Cloud Security Alliance, "Top Threats to Cloud Computing: Pandemic 11 Deep Dive", ottobre 2023.

Consigli e best practice

Una strategia di gestione e automazione estesa all'intera azienda consente di tenere il passo con l'evoluzione della sicurezza, dei rischi e dei requisiti di conformità. Adottare una strategia di gestione e automazione coerente in tutto il cloud ibrido contribuisce ad aumentare l'agilità, la ripetibilità, la coerenza e semplifica i processi di verifica.



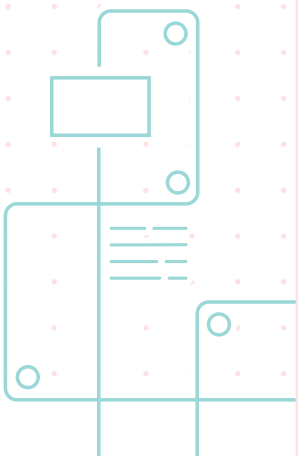
Una strategia di automazione unificata aiuta a ridurre il rischio di introdurre errori di configurazione ed errori manuali. L'automazione e la gestione permettono di razionalizzare e standardizzare l'amministrazione dell'infrastruttura, dello sviluppo applicativo e delle operazioni di sicurezza, e migliorano così la protezione, la conformità e il controllo delle modifiche. In questo modo le aziende possono:

Configurare in modo coerente le risorse in base a criteri preapprovati e gestirli in modo proattivo e reiterativo durante l'intero ciclo di vita.

Identificare rapidamente i sistemi che richiedono patch o una riconfigurazione.

Applicare le patch più facilmente o modificare le impostazioni di sistema in conformità a baseline definite, in modo coerente e su più sistemi.

Semplificare i processi di verifica e risoluzione dei problemi grazie a registri di interventi che si compilano automaticamente.



Per gestire la sicurezza di ambienti operativi, applicazioni, operazioni e ambienti cloud ibridi sempre più complessi, le aziende moderne puntano sull'automazione dell'IT. **Red Hat Ansible Automation Platform** è una piattaforma di automazione end to end che offre un framework coerente pensato per le aziende con cui creare e gestire l'automazione dell'IT in maniera scalabile, mettendo sempre la sicurezza al primo posto. Contribuisce a migliorare l'efficienza e la produttività, contiene i rischi e i costi, permette ai team di automatizzare e standardizzare la sicurezza e la conformità in tutta l'azienda in maniera ripetibile, e consente di rispondere alle minacce in modo coordinato e tempestivo grazie ai contenuti di automazione certificati e al supporto di livello enterprise sempre disponibile di Red Hat.

Red Hat Ansible Automation Platform fornisce funzionalità automatizzate fondamentali per far fronte alle minacce e agli attacchi, tra cui gestione della configurazione, applicazione di patch e correzione. Inoltre, Red Hat Ansible Automation Platform può fungere da punto di integrazione per le soluzioni di sicurezza. Grazie ai contenuti di partner certificati, come CyberArk, IBM e Palo Alto Networks, la piattaforma si può anche utilizzare per gestire e integrare in maniera automatizzata un gran numero di tecnologie di sicurezza esterne.

Integrare la piattaforma e i processi di automazione con tecniche di gestione delle identità e controllo degli accessi assicura che solo il personale autorizzato possa eseguire le attività di automazione. Scegli una piattaforma di automazione di facile utilizzo. L'adozione di una piattaforma e di un linguaggio di automazione intuitivi migliora i seguenti aspetti:

Visibilità. Chiunque è in grado di comprendere tutte le attività di automazione.

Ripetibilità. Una piattaforma e un linguaggio accessibili consentono a tutto il personale approvato di sfruttare l'automazione in modo efficace ed efficiente.

Collaborazione. Le attività di automazione si possono condividere all'interno dell'organizzazione in modo da non svolgere più volte le stesse attività.

Controllo. I diversi team sono in grado di verificare le attività di automazione e visualizzare i registri per svolgere gli audit.

Azioni strategiche

Segui questi suggerimenti per favorire l'automazione della sicurezza:

Inizia da un singolo progetto.
Procedi in maniera graduale. Scegli un solo progetto o un numero ristretto di attività da cui partire.

Scegli attività ripetitive.
Automatizza attività eseguite in modo ripetitivo, tra cui la gestione della configurazione, la gestione del pacchetto software e delle patch, l'identificazione delle vulnerabilità e la relativa correzione e l'applicazione dei criteri.

Scegli l'automazione continua.
Implementa l'automazione e misura i risultati per un'adattabilità costante.

Pianifica la scalabilità dell'automazione con una piattaforma end to end.
Assicurati che i processi di automazione siano sempre verificabili e condivisibili cosicché vadano a vantaggio di tutta l'organizzazione e adotta una piattaforma di automazione end to end di livello enterprise per garantire la scalabilità dell'automazione.

Capitolo 6

Inizia il tuo percorso

La sicurezza del cloud ibrido è una responsabilità condivisa in tutte le organizzazioni. Qualsiasi sia il grado di transizione al cloud ibrido raggiunto dalla tua azienda, Red Hat può aiutarti a distribuire un ambiente cloud ibrido incentrato sulla sicurezza.

Grazie alle funzionalità di sicurezza integrate, l'ampia gamma di software open source per ambienti di produzione offerta da Red Hat fornisce tutti gli strumenti e le piattaforme necessari a superare le sfide presenti e future in materia di sicurezza e conformità. Red Hat propone inoltre un supporto di livello enterprise, corsi di formazione pratici e servizi di esperti per aiutare a creare e gestire gli ambienti cloud ibridi in modo efficiente e sicuro.

Scopri l'approccio di Red Hat alla sicurezza del cloud ibrido

Consulta le seguenti risorse per scoprire di più sull'approccio di Red Hat alla sicurezza e alla conformità del cloud ibrido.

- Panoramica sulla sicurezza del cloud ibrido
- Valutazione della sicurezza del cloud ibrido
- Approcci alla sicurezza per gli ambienti cloud ibridi
- Aumenta la sicurezza del cloud ibrido

Informazioni su Lucy Huh Kerner, Director, Security Global Strategy and Evangelism, Red Hat
Responsabile della strategia tecnica e di go to market per la sicurezza dell'intero portafoglio di prodotti Red Hat, Lucy Huh Kerner aiuta a sviluppare la sicurezza a livello globale. Aiuta inoltre a realizzare e distribuire contenuti tecnici correlati alla sicurezza per esperti di settore, clienti, partner, analisti e per la stampa e ha partecipato a numerosi eventi e conferenze in qualità di esperta in materia di sicurezza. Lucy vanta un'esperienza comprovata di oltre 20 anni come software and hardware development engineer, solutions architect e global security strategist, ruoli che le hanno consentito di approfondire vari aspetti della sicurezza informatica.

ITALIA
it.redhat.com
italy@redhat.com

EUROPA, MEDIO ORIENTE, E AFRICA (EMEA)
00800 7334 2835
it.redhat.com
europe@redhat.com

facebook.com/RedHatItaly
twitter.com/RedHatItaly
linkedin.com/company/red-hat

it.redhat.com