Focus sulla sicurezza: Il costo dell'errore umano e i vantaggi dell'automazione

Perché gli enti della pubblica amministrazione stanno rivalutando gli approcci manuali alla gestione della sicurezza e in che modo l'automazione intelligente contribuisce a prevenire potenziali minacce causate da vulnerabilità

Avanti

In questo ebook:

01 Introduzione: la crescente minaccia dei crimini informatici

I crimini informatici sono in aumento. Il numero di incidenti di sicurezza informatica è infatti aumentato del 15,5% nel 2021, mentre la quantità di violazioni materiali è cresciuta del 24,5%.[1] Nonostante ciò, il 34% delle organizzazioni del settore pubblico afferma di non essere adeguatamente preparato al panorama delle minacce in rapida evoluzione.[1]

In uno scenario in cui gli enti della pubblica amministrazione adottano nuove tecnologie e si adattano a modelli ibridi di lavoro, anche i criminali informatici sviluppano nuove abilità. La forza lavoro e le risorse di elaborazione sono più distribuite e la rapida evoluzione delle infrastrutture IT fornisce ai malintenzionati nuove opportunità per sfruttare vulnerabilità e lacune nella sicurezza, con un conseguente aumento dei costi organizzativi legati alle violazioni dei dati. Questo tipo di ambienti comporta più rischi anche per le organizzazioni con un solido approccio alla sicurezza.

Sicurezza proattiva contro i criminali informatici

Mentre i criminali informatici elaborano nuovi metodi per violare dati e sistemi protetti, le organizzazioni subiscono pressioni interne ed esterne legate alla necessità di adottare sistemi di protezione più strategici e proattivi nei confronti degli attacchi informatici. Di fatto, le loro misure per la privacy e la sicurezza dei dati devono soddisfare normative e regole più estese.

Questa tendenza che vede l'aumento di normative per la privacy e la sicurezza si applica a più settori e aree geografiche. Il Regolamento generale per la protezione dei dati personali (RGPD), ad esempio, definisce regole rigorose in materia di raccolta, utilizzo e protezione dei dati. Il Cybersecurity Act di Singapore delinea un framework secondo il quale i proprietari di infrastrutture di informazioni critiche sono tenuti a seguire procedure consigliate in ambito di governance, controllo degli accessi, rilevamento e risposta alle minacce e altri ambiti. Anche la Dirección Nacional de Ciberseguridad stabilisce normative per proteggere le infrastrutture di informazioni critiche e migliorare la prevenzione, il rilevamento, la risposta e il ripristino di incidenti di sicurezza a livello nazionale. Inoltre, gli enti della pubblica amministrazione statunitense devono adottare architetture zero trust per rispettare gli obiettivi di sicurezza informativa federali entro la fine del 2024.

Consolidamento delle difese

Le organizzazioni che desiderano potenziare la sicurezza informatica devono innanzitutto identificare le vulnerabilità esistenti. Troppo spesso gli errori umani e la disinformazione possono vanificare le strategie in atto, sebbene siano considerate complete. Anche un piccolo errore, se sfugge al controllo, può implicare dei rischi per i sistemi, aggravando problemi già complessi. Di conseguenza, le organizzazioni stanno promuovendo l'adozione dell'automazione per migliorare l'affidabilità e ridurre i rischi nella strategia di sicurezza.

In questo ebook, analizzeremo l'impatto degli errori umani sulla lotta ai crimini informatici e scopriremo in che modo l'automazione delle principali strategie di mitigazione del rischio può rafforzare la sicurezza informatica, riducendo al contempo il volume di attività dispendiose in termini di tempo che gravano sui team IT.

Il costo globale della criminalità informatica

24,5%

Aumento delle violazioni materiali nel 2021[1]

4,35 miliardi di dollari

Costo medio globale di una violazione dei dati[2]

60%

Percentuale di organizzazioni che hanno aumentato i prezzi dei propri servizi o prodotti a causa di una violazione dei dati[2]

1. ThoughtLab. "Cybersecurity Solutions for a Riskier World", 2022
2. IBM. "Cost of a Data Breach Report 2022", luglio 2022.

02 L'importanza di adottare strategie di sicurezza efficaci

Gli esseri umani commettono errori

Anche i membri dei team IT spesso sottovalutano o fraintendono le vulnerabilità dei sistemi e i rischi di sicurezza che ne derivano. L'incapacità di valutare accuratamente i rischi può comportare costi significativi per le organizzazioni.

Facciamo un esempio: il firewall smette di funzionare e costringe gli ingegneri ad aggiornare manualmente un criterio in fretta e furia. La modifica ripristina il funzionamento ma introduce anche un nuovo vettore di attacco che può essere sfruttato dai criminali informatici.

In questo scenario, la modifica manuale e affrettata della configurazione del firewall potrebbe causare diversi effetti negativi, tra cui compromissione dei dati, violazione degli standard di settore e delle normative vigenti sulla sicurezza dei dati, interruzione del servizio e downtime del sistema, il tutto a spese dell'organizzazione.

Se gestite manualmente infatti, è possibile che le numerose attività di sicurezza, dal patching delle applicazioni all'aggiornamento dei firewall alla configurazione e applicazione dei privilegi di amministrazione, non funzionino come previsto. A fronte di criminali informatici sempre più abili nell'identificare e sfruttare le vulnerabilità, affidarsi esclusivamente a operazioni manuali per queste attività può avere conseguenze deleterie o irrimediabili.

La carenza di talenti aggrava le falle di sicurezza

La mancanza di personale qualificato in materia di sicurezza informatica non fa che aumentare la probabilità di errore umano durante le attività manuali. Semplicemente, non ci sono abbastanza figure con le competenze e la formazione necessarie per valutare e affrontare i rischi per la sicurezza. Secondo il Cybersecurity Workforce Study (ISC)[2], mancano più di 2,72 milioni di esperti IT per colmare il divario nella sicurezza informatica a livello globale.[3]

Questa carenza cronica di professionisti della cybersecurity rende più difficile per le organizzazioni gestire adeguatamente i rischi. I team IT sono oberati di lavoro e non hanno il tempo di applicare le procedure di sicurezza all'interno dell'organizzazione, figuriamoci crearle.

L'automazione al servizio dei team di sicurezza

Nella lotta contro la criminalità informatica, l'aumento del rischio dovuto a procedure di sicurezza manuali e carenza di competenze all'interno delle organizzazioni è ormai una questione imprescindibile. Le soluzioni di automazione offrono riscontri promettenti: come vedremo più avanti, l'automazione dei processi di sicurezza garantisce la coerenza, la precisione e la scalabilità indispensabili per l'organizzazione.

I rischi delle misure di sicurezza manuali

"Le organizzazioni che hanno completato l'adozione di progetti di AI e automazione per la gestione della sicurezza sono stati in grado di rilevare e contenere le violazioni molto più rapidamente rispetto alle organizzazioni che non ne fanno uso".[4]

3. (ISC)[2] Cybersecurity Workforce Study. "A Resilient Cybersecurity Profession Charts the Path Forward", 2021.
4. IBM. "Cost of a Data Breach Report 2022", luglio 2022.

03 Gestione dei rischi e sfide comuni

Necessità di una migliore gestione dei rischi per gli enti della pubblica amministrazione

Per garantire la riservatezza, l'integrità e la disponibilità delle informazioni ufficiali, gli enti della pubblica amministrazione devono essere in grado di individuare e gestire i rischi in modo accurato ed efficiente. Di conseguenza, il profilo di rischio e il livello sicurezza di un'organizzazione necessitano di una certa flessibilità per adeguarsi alle minacce in continua evoluzione. L'automazione delle operazioni è fondamentale per poter rispondere rapidamente a questi cambiamenti.

Ostacoli all'evoluzione delle procedure di sicurezza

Nell'ambito delle iniziative per migliorare la sicurezza, gli enti della pubblica amministrazione incontrano diverse difficoltà, soprattutto per quanto riguarda la gestione del cambiamento. I dubbi più frequenti riguardano:

- Come ampliare il team per implementare nuove iniziative di sicurezza informatica
- Come supportare i diversi reparti dell'organizzazione per garantire il rispetto dei nuovi protocolli di sicurezza
- Cosa fare per rendere più sicuri i sistemi esistenti che forniscono i servizi essenziali adottando al contempo le strategie di sicurezza all'avanguardia di cui l'organizzazione ha bisogno
- Possibilità di implementare strategie zero trust e simili su architetture consolidate

Tuttavia, le organizzazioni non dovrebbero vivere come un peso le considerazioni sul panorama della sicurezza in continua evoluzione, ma piuttosto considerarle un'opportunità per rivalutare le procedure di sicurezza e implementare protocolli più rigorosi.

Le sfide più comuni legate alla sicurezza informatica

38%

Restare al passo con le minacce in continua evoluzione[5]

34%

Sensibilizzare su rischi e comportamenti[5]

31%

Rafforzare la sicurezza informatica all'interno dell'organizzazione[5]

30%

Garantire la formazione in materia di sicurezza informatica[5]

30%

Gestire le conseguenze legali/finanziare delle violazioni dei dati[5]

5. "State of the Channel 2021". CompTIA, agosto 2021.

04 Livelli di sicurezza avanzati grazie all'automazione

Tematiche comuni nelle normative in materia di sicurezza

La riservatezza dei dati, il controllo degli accessi e la protezione, il rilevamento e la risposta agli incidenti sono elementi che accomunano le normative e le iniziative per la sicurezza informatica in qualsiasi settore e area geografica. Sebbene alcune normative forniscano dettagli sull'implementazione, la maggior parte si limita a definire linee guida e risultati attesi, lasciando alle organizzazioni il compito di individuare le modalità migliori per soddisfare i regolamenti in base alla situazione attuale, alle dimensioni dell'organico e all'infrastruttura.

L'automazione della sicurezza aiuta gli enti della pubblica amministrazione e le organizzazioni a combattere la criminalità informatica e a rispettare le normative. Grazie all'automazione delle attività periodiche e ripetitive, i team della sicurezza informatica possono concentrarsi su attività più importanti e strategiche. Inoltre, l'automazione riduce il sovraccarico dei team IT eliminando compiti e volumi di lavoro che aumentano le probabilità di errore umano e i rischi per la sicurezza.

Team più connessi grazie all'automazione della sicurezza

L'automazione della sicurezza implica una serie di procedure che collegano i team e i domini dell'organizzazione per gestire meglio i rischi, difendersi dalle minacce informatiche e contenere gli incidenti. Ad esempio, gli analisti della sicurezza, i team IT operativi e gli amministratori di rete possono, rispettivamente, automatizzare i processi di risposta e correzione degli incidenti, applicare automaticamente le patch ai sistemi per garantire la conformità e impostare e gestire i controlli degli accessi alla rete.

Inoltre, l'automazione favorisce una collaborazione più efficiente tra i team IT e della sicurezza e le altre funzioni dell'organizzazione interessate dalle normative in materia, come le risorse umane, l'assistenza clienti e l'ufficio legale. Ad esempio, la maggior parte delle aziende è tenuta verificare i controlli di sicurezza e segnalare gli incidenti informatici per garantire la conformità ai requisiti legali. Gli addetti alle attività di auditing richiedono prove di conformità, ma spesso non interagiscono direttamente con i sistemi di sicurezza dell'organizzazione. L'automazione consente di integrare i sistemi di registrazione esterni e registrare le azioni per fornire tutti i report e le prove necessarie.

Automazione per la gestione dei rischi

L'automazione dei processi chiave all'interno dell'organizzazione aiuta a rafforzare la sicurezza attiva e passiva. Nelle sezioni seguenti esamineremo diverse aree in cui l'automazione della sicurezza garantisce la conformità alle normative e produce effetti concreti sulle aziende, indipendentemente dall'area geografica.

Risposta e correzione degli incidenti

Nel 2022, il tempo medio per identificare e arginare una violazione dei dati è stato di 277 giorni.[6]Riuscire a ridurre questo intervallo a 200 giorni, o anche meno, può risultare in un taglio medio delle spese del 26,5%.[6] Ciononostante, il rilevamento e la correzione delle violazioni su più piattaforme, strumenti e ambienti possono risultare complessi, dispendiosi in termini di tempo e soggetti a errori, se eseguiti manualmente.

In presenza di una violazione, occorre adottare le misure necessarie per contenerla, intervenendo tempestivamente e su tutti i sistemi interessati. Tuttavia, le azioni di risposta spesso richiedono diverse attività manuali da eseguire su sistemi non connessi, che rallentano l'intervento e aumentano la durata dell'esposizione alla minaccia.

L'automazione della sicurezza permette di reagire agli imprevisti più velocemente, codificando le azioni di correzione in playbook ripetibili e preapprovati. È possibile accelerare attività come il blocco degli indirizzi IP o i domini di origine dell'attacco, consentendo il flusso del traffico legittimo, il congelamento delle credenziali compromesse e l'isolamento dei carichi di lavoro sospetti, per analizzarli ulteriormente, allo scopo di minimizzare i danni.

Applicazione di patch e aggiornamenti di sistema

Numerosi standard di sicurezza informatica consigliano alle organizzazioni di applicare regolarmente le patch a sistemi e applicazioni e di effettuare gli aggiornamenti periodici per prevenire gli attacchi. Purtroppo, però, l'applicazione di patch e gli aggiornamenti manuali sono sempre soggetti a errori umani e richiedono molto tempo, specialmente nelle aziende più grandi.

L'importanza di tempi di risposta rapidi

277 giorni

Tempo medio necessario per identificare e arginare una violazione dei dati nel 2022[6]

26,5%

Riduzione dei costi per le violazioni dei dati rilevate e identificate entro 200 giorni[6]

I flussi di lavoro automatizzati sono particolarmente indicati per l'applicazione di patch. Invece di affidarsi a test manuali, controlli preliminari e installazione delle patch, le organizzazioni possono automatizzare la verifica e la valutazione per semplificare e ottimizzare la procedura e garantire un adeguato livello di sicurezza in background.

Gestione di credenziali e privilegi

Il furto o la manomissione delle credenziali rappresentano una delle cause più comuni di violazioni dei dati.[6] La centralizzazione e il controllo degli accessi privilegiati e delle credenziali contribuiscono a ridurre i rischi e a garantire la conformità alle normative in materia di privacy e sicurezza dei dati,

in quanto entrambi sfruttano il principio dei privilegi minimi per fornire agli utenti l'accesso solo a ciò di cui hanno effettivamente bisogno. Sebbene richieda il controllo e la rivalutazione dei diritti di accesso correnti per ogni utente, questo approccio aiuta a ridimensionale le conseguenze del furto o della manomissione delle credenziali.

La memorizzazione delle credenziali di accesso a livello centrale elimina la necessità di inserirle direttamente nelle applicazioni ed esporle a maggiori vulnerabilità. I flussi di lavoro automatizzati per la gestione degli accessi privilegiati rendono il processo più gestibile, affidabile e coerente e gettano le basi per architetture e approcci zero trust.

Conformità e applicazione dei criteri

Gli errori di configurazione rappresentano la causa principale del 44% delle maggiori violazioni di sicurezza delle organizzazioni.[7] I sistemi configurati in modo errato sono più soggetti agli attacchi. Se le organizzazioni non dispongono di accurati controlli delle modifiche, anche i sistemi configurati correttamente al momento del provisioning possono diventare più vulnerabili nel tempo.

L'applicazione dei criteri sull'intero ciclo di vita dei sistemi e delle applicazioni assicura una corretta configurazione iniziale e il mantenimento delle impostazioni nel tempo. Grazie all'automazione, è possibile raggiungere questo obiettivo rapidamente e in modo scalabile, aumentando al contempo l'uniformità di sistemi e ambienti distribuiti. Inoltre, l'automazione applicata ai processi di controllo delle modifiche consente di verificare l'approvazione delle richieste di modifica, registrare le attività e generare report a scopo di audit.

6. IBM. "Cost of a Data Breach Report 2022", luglio 2022.
7. ThoughtLab. "Cybersecurity Solutions for a Riskier World", 2022

Architetture zero trust

Procedendo con l'automazione dei processi descritti in precedenza, le organizzazioni acquisiscono preziose esperienze e gettano le basi per un'architettura zero trust. Zero trust è un modello architetturale che gestisce la sicurezza a livello di ciascuna risorsa invece che applicarla solo al perimetro di rete. Nessun attore, sistema, rete o sistema che opera dentro o fuori dal perimetro di sicurezza è considerato implicitamente affidabile. Per consentire la connessione tra un utente o soggetto e una risorsa, la fiducia viene stabilita in modo esplicito solo quando la sessione viene autenticata e autorizzata.

La gestione degli accessi e delle identità è al centro delle architetture zero trust. Ogni soggetto che vuole interagire con una risorsa deve richiedere l'accesso per quella specifica interazione. I rischi ad essa collegati vengono valutati prima che l'accesso venga autorizzato. La comprensione dell'identità e degli attributi del soggetto è indispensabile ai fini di questa valutazione. È necessario stabilire le informazioni contestuali, ad esempio chi inoltra la richiesta di accesso, quali sono le risorse coinvolte, qual è lo scopo della transazione e in che modo l'accesso deve essere limitato.

Dopo aver preso le decisioni necessarie riguardo all'accesso, bisogna archiviare, gestire, curare e aggiornare le identità e i rispettivi attributi in modo sicuro e uniforme. Per amministrare queste informazioni, la maggior parte delle aziende impiega uno o più sistemi di gestione degli accessi privilegiati e delle identità. È inoltre necessario riesaminare continuamente le decisioni che riguardano gli accessi per garantire che siano ancora valide con il passare del tempo.

Poiché è prevista una valutazione del rischio per ciascuna interazione, gli approcci zero trust richiedono la raccolta di una grande quantità di dati e informazioni da tutta l'infrastruttura e l'organizzazione. È in questa fase che l'automazione diventa fondamentale. In primo luogo, il numero di interazioni è semplicemente troppo elevato per essere gestito e valutato manualmente dal personale IT, e risulterebbe impossibile concedere l'accesso alle risorse in modo tempestivo.

In secondo luogo, l'automazione può aiutare a raccogliere dati da sistemi diversi all'interno dell'organizzazione. Ad esempio, se un dipendente vuole accedere a un'applicazione interna, potrebbe essere necessario raccogliere e verificare le informazioni professionali da un software per la gestione delle risorse umane, i dati sull'identità da un sistema IT e le informazioni sullo stato di aggiornamento e sulla posizione dal suo computer, a seconda dei casi. Le piattaforme di automazione collegano sistemi e domini che di solito non interagiscono o non possono interagire tra loro, consentendo quindi di recuperare e analizzare le informazioni in modo semplice e rapido e di inviarle a un sistema Security Information and Event Management (SIEM) e ad altri sistemi centralizzati di sicurezza informatica e gestione eventi in base alle esigenze aziendali.

Infine, l'automazione consente di rispondere in modo dinamico agli eventi e alle modifiche di stato degli utenti. Se un utente lascia l'azienda o cambia ruolo all'interno dell'organizzazione, è possibile utilizzare l'automazione basata sugli eventi per aggiornare gli accessi in tutti i sistemi in tempo reale anziché attendere un'azione manuale.

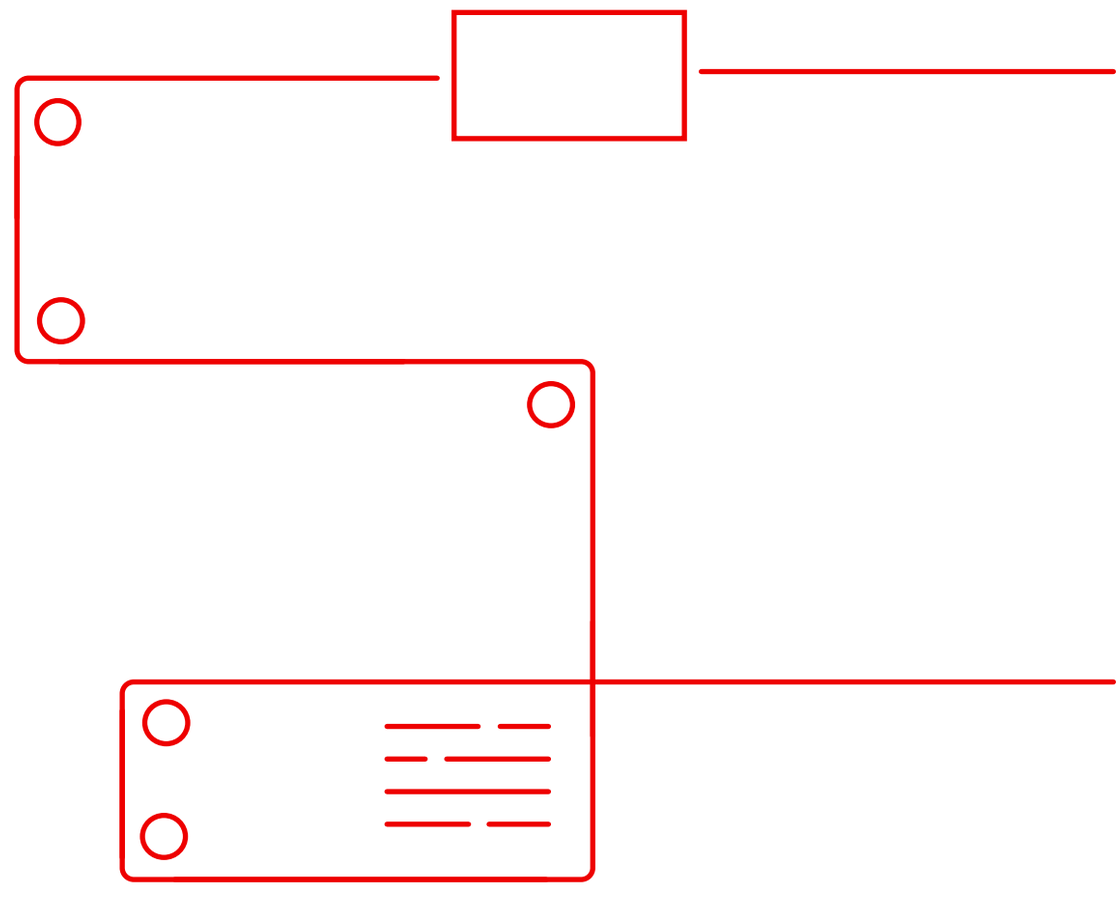
Vantaggi degli approcci zero trust

20,5%

Percentuale di risparmio sui costi delle violazioni dei dati per le organizzazioni che adottano il modello zero trust[8]

1,65 milioni di dollari

Risparmio medio sui costi delle violazioni dei dati associati a un modello zero trust in fase matura rispetto all'assenza di zero trust[8]



8. IBM. "Cost of a Data Breach Report 2022", luglio 2022.

05 Il contributo di Red Hat nell'approccio alla sicurezza informatica

Misure di sicurezza informatica pronte per il futuro

Grazie a un modello di maturità della sicurezza informatica basato sull'automazione, è possibile adottare misure pratiche per sostituire rapidamente e con tutte le iterazioni necessarie i processi manuali, gestire i rischi e migliorare il profilo di sicurezza. Le soluzioni Red Hat® aiutano ad automatizzare i processi manuali già esistenti per ridurre il rischio di sviste dovute a team IT sovraccarichi e con personale ridotto nell'organizzazione. I nostri prodotti open source offrono flessibilità e scalabilità in ambienti e architetture cloud e contribuiscono a potenziare subito la sicurezza e a far fronte alle incertezze del futuro.

Red Hat Ansible Automation Platform

Red Hat Ansible® Automation Platform utilizza un linguaggio di automazione leggibile in chiaro che trasforma processi manuali complessi in flussi di lavoro automatizzati. La nostra piattaforma consente ai team IT di automatizzare e integrare i protocolli di sicurezza in tutta l'azienda, rilevare le minacce e rispondere in modo coordinato e unificato sfruttando contenuti di automazione curati e certificati. È inoltre possibile automatizzare:

- Aggiornamenti e patch per vulnerabilità ed esposizioni comuni (Common Vulnerabilities and Exposures, CVE).
- Deployment del controllo delle applicazioni.
- Processi di backup, ripristino e verifica.

Ansible Automation Platform fornisce un framework enterprise stabile e incentrato sulla sicurezza per la creazione e la gestione dell'automazione IT su larga scala, dal cloud ibrido agli ambienti edge. Questa soluzione consente a tutti gli utenti di un'organizzazione, dai team operativi e di sviluppo fino a quelli che si occupano di sicurezza e della rete, di creare, condividere e gestire contenuti e playbook di automazione. I responsabili IT possono definire linee guida sulle modalità di applicazione dell'automazione per i singoli team e gli autori delle automazioni possono preparare attività che si avvalgono delle conoscenze esistenti.

Inoltre, Ansible Automation Platform utilizza i contenuti inclusi di partner certificati come CyberArk, IBM e Splunk per aggregare diverse soluzioni e automatizzare la gestione e l'integrazione delle tecnologie di sicurezza.

Scopri di più su Red Hat Ansible Automation Platform ›

Red Hat Enterprise Linux

Red Hat Enterprise Linux offre una base da cui è possibile espandere le applicazioni esistenti e distribuire le tecnologie emergenti in ambienti bare metal, virtuali, cloud ed edge con funzionalità di sicurezza uniformi.

Red Hat Enterprise Linux adotta un approccio pratico per affrontare le tre principali problematiche legate alla sicurezza:

- Mitigazione: gestire la sicurezza e ridurre il rischio di violazioni del firewall per preservare i dati, i sistemi e la reputazione dell'organizzazione.
- Protezione: automatizzare i controlli di sicurezza e mantenerli nel tempo, in modo scalabile e con downtime minimi.
- Conformità: semplificare gli standard di conformità delle organizzazioni con ambienti altamente regolamentati.

Red Hat Enterprise Linux include inoltre criteri di sicurezza integrati e allineati a normative e standard quali Common Criteria (CC), Federal Information Processing Standard (FIPS) 140 e Secure Technical Implementation Guidelines (STIG), per migliorare la gestione del rischio applicando automaticamente e in modo uniforme i controlli di sicurezza ai nuovi servizi digitali.

Scopri di più su Red Hat Enterprise Linux ›

Red Hat

Indietro

Potenzia la sicurezza con Red Hat

Red Hat è qui per aiutarti a incrementare la sicurezza dei tuoi servizi digitali

Applica l'automazione agli standard e agli orientamenti normativi e gestisci meglio i rischi grazie alle integrazioni di sicurezza automatizzate di Red Hat.

Contattaci subito per saperne di più >