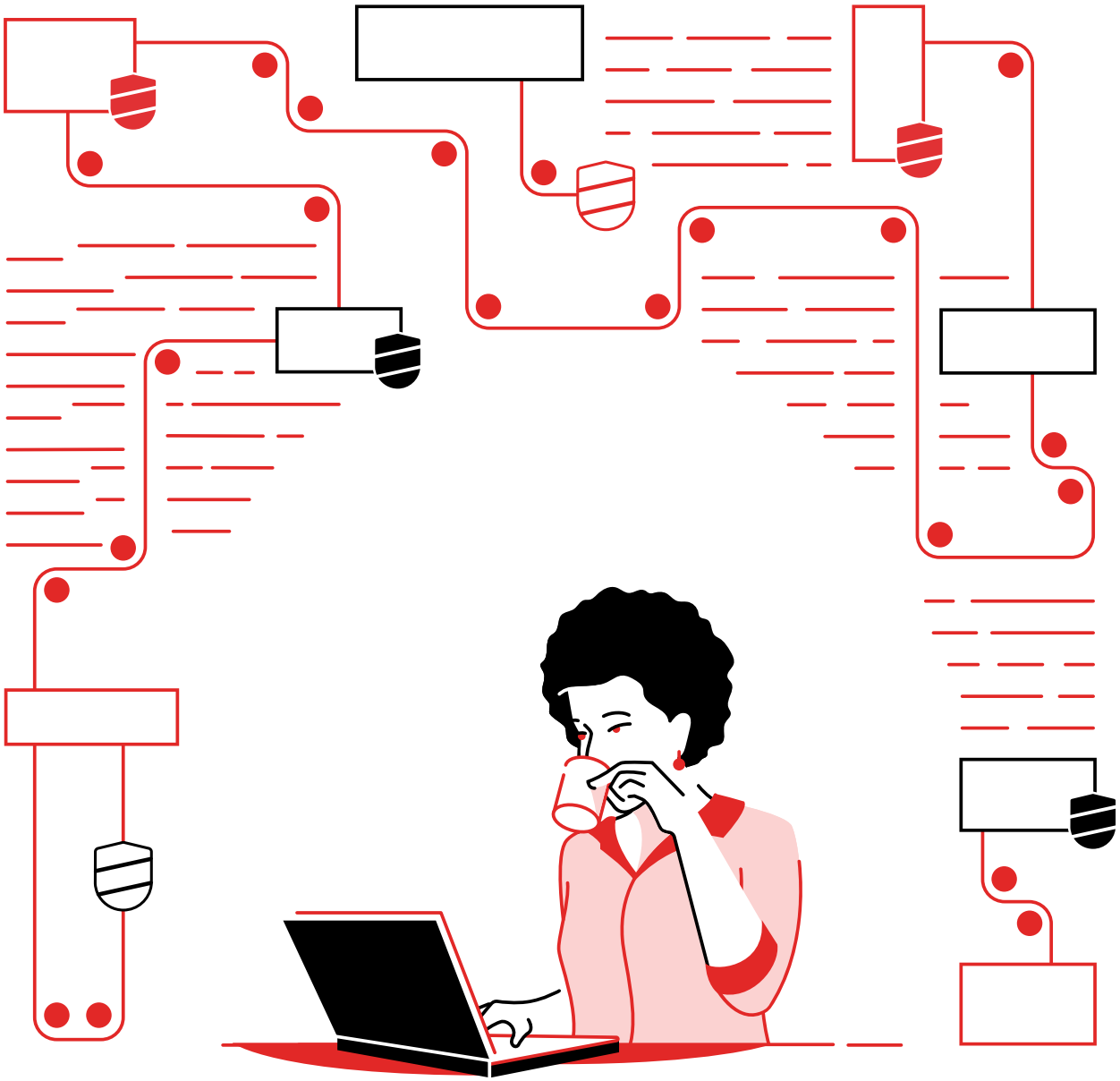
Semplifica il tuo centro operativo di sicurezza

Migliora velocità, tempi e sicurezza, con una piattaforma di automazione unificata



Red Hat

Contenuti

L'importanza della sicurezza informatica

La sicurezza costituisce un problema importante per la maggior parte delle aziende. Le minacce informatiche costituiscono una grave preoccupazione per il 33% dei CEO,[1] e per ottime ragioni: negli ultimi due anni il 32% delle aziende ha subito un grave attacco informatico.[2]

Pertanto, proteggere l'azienda è fondamentale, ma spesso può presentare ostacoli all'apparenza insormontabili. I team dedicati alla sicurezza informatica devono predisporre, gestire e adattare ambienti complessi, utilizzando strumenti e servizi di fornitori diversi, che spesso sono in concorrenza fra loro. Le offerte aumentano di anno in anno e, a mano a mano che il panorama della sicurezza si evolve, i team devono continuamente cercare, valutare e integrare nuovi prodotti.

Come se non bastasse, il numero, la gravità e il costo delle violazioni continuano ad aumentare. La probabilità di subire una violazione entro i prossimi due anni è del 29,6%, in aumento rispetto al 22,6% del 2014.[3] Dal 2018 al 2019, il numero medio dei record interessati da una singola violazione dei dati è aumentato del 3,9%,[3] mentre il costo medio di una violazione dei dati è salito a 3,92 milioni di dollari, nel 2019.[3]

In molte aziende le violazioni dei dati vengono ancora gestite manualmente. Quando è necessario un intervento umano, le attività correlate alla sicurezza possono diventare lunghe, ripetitive e ad alta probabilità di errore, generando un sovraccarico di lavoro per i team di sicurezza, che si ritrovano a gestire un numero crescente di segnalazioni provenienti da diversi strumenti. Infatti, il 60% dei team di sicurezza riceve più di 5.000 segnalazioni al giorno e il 16% ne riceve più di 100.000 al giorno.[4]

Inoltre, all'aumentare delle dimensioni e della complessità dell'infrastruttura, identificare le vulnerabilità e verificare le violazioni diventa sempre più difficile. Molti degli strumenti di sicurezza non sono integrabili, e ciò causa un ulteriore incremento del carico di lavoro del personale di sicurezza, e un aumento del tempo necessario per analizzare gli incidenti e rispondere adeguatamente. Nel 2019, il tempo medio necessario per identificare e contenere una violazione dei dati era di 279 giorni, il 4,9% in più rispetto al 2018.[3] Inoltre, non è facile trovare personale esperto da inserire nel team di sicurezza per tenere il passo; infatti, nel 2019, il 39% delle aziende ha segnalato una carenza di competenze in materia di sicurezza informatica.[2] Infine, i budget per le attività di sicurezza informatica sono limitati. Solo il 33% delle aziende dichiara di avere a disposizione fondi sufficienti per garantire un alto livello di resilienza informatica.[5]

Di conseguenza, i team di sicurezza solitamente esaminano e rispondono solo al 48% degli avvisi che ricevono e risolvono solo il 50% delle minacce effettive,[4] lasciando molte aziende vulnerabili agli attacchi.

77% Percentuale delle aziende che prevedono di incrementare l'automazione per semplificare e accelerare i tempi di risposta nei propri ecosistemi di sicurezza.[4]

Le conseguenze di una sicurezza inefficace

Il numero, la gravità e il costo delle violazioni continuano ad aumentare.

3,92 milioni di dollari
Costo medio di una violazione dei dati nel 2019[3]

279 giorni
Tempo medio necessario per identificare e contenere una violazione dei dati nel 2019[3]

1,22 milioni di dollari
Risparmio sui costi ottenibile riuscendo a identificare e contenere una violazione

200 giorni
o meno[3]

29,6%
Probabilità di subire una violazione entro due anni[3]

50%
Proporzione delle minacce effettive eliminate[4]

1 *PWC, "23rd Annual Global CEO Survey: Navigating the rising tide of uncertainty", 2020.* pwc.com/ceosurvey.
2 *Harvey Nash and KPMG, "CIO Survey 2019: A Changing Perspective", 2019.* home.kpmg/xx/en/home/insights/2019/06/harvey-nash-kpmg-cio-survey-2019.html.
3 *IBM Security, "2019 Cost of a Data Breach Report", 2019.* ibm.com/security/data-breach.
4 *Cisco, "Cisco Benchmark Study: Securing What's Now and What's Next", febbraio 2020.* cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html.
5 *Ponemon Institute, sponsorizzato da IBM Security, "The Cyber Resilient Organization", aprile 2019.* ibm.com/account/reg/us-en/signup?formid=urx-37792.

Cos'è l'automazione della sicurezza?

L'automazione della sicurezza comporta l'automazione delle attività manuali necessarie per mantenere il livello di sicurezza dell'azienda, e richiede varie procedure, che abbiamo suddiviso in quattro categorie generali:

Risposta e correzione
Attività basate su eventi che richiedono la collaborazione e/o le indicazioni di un analista della sicurezza

Operazioni di sicurezza
Attività basate su eventi e processi quotidiani eseguiti dai team IT sull'infrastruttura di sicurezza

Conformità alle normative di sicurezza
Attività con lo scopo di garantire la conformità dell'infrastruttura alle normative e ai criteri di sicurezza

Potenziamento
Applicazione dei criteri di sicurezza all'infrastruttura, con finalità e obiettivi specifici

Scopri come garantire sicurezza e conformità alle normative

Per scoprire come sfruttare l'automazione per aumentare i livelli di sicurezza e garantire la conformità alle normative, leggi queste risorse:

- **Ebook: Incrementa la sicurezza del cloud ibrido**
- **Panoramica: L'importanza dell'automazione di sicurezza e compliance**
- **Scheda tecnica: Red Hat Services: Automazione dei processi di sicurezza e compliance**

Questo ebook illustra come automatizzare le attività di risposta e correzione, così come le operazioni di sicurezza.

Vantaggi dell'automazione per le operazioni di sicurezza e le attività di risposta e correzione

Aumenta velocità ed efficienza

L'automazione semplifica le attività ed elimina la necessità di intervenire manualmente, accelerando le operazioni di sicurezza e consentendo al personale di dedicarsi a iniziative più importanti. Consente inoltre di ridurre la complessità dell'infrastruttura IT: il 40% delle aziende con alti livelli di automazione dichiara infatti di utilizzare il numero appropriato di soluzioni e tecnologie di sicurezza.[6]

Incrementa la sicurezza secondo le necessità

Applicando l'automazione a tutti i livelli dell'infrastruttura di sicurezza, è possibile aumentare la coerenza e adottare un approccio più olistico alla sicurezza. Ciascun membro del team può gestire un maggior numero di strumenti, dispositivi e sistemi, a seconda delle esigenze. L'automazione riduce inoltre il rischio di errore umano, aumentando la precisione.

Riduci il rischio di violazioni e dei costi associati

Le aziende che implementano l'automazione su vasta scala riescono a prevenire più efficacemente gli incidenti di sicurezza e le interruzioni dell'attività aziendale.[6] Il deployment completo dell'automazione della sicurezza consente di ridurre del 95% il costo medio di una violazione.[7] Proprio per questo, il 52% delle aziende ha automatizzato almeno in parte le attività di sicurezza e un ulteriore 36% prevede di farlo nei prossimi 24 mesi.[7]

6 Ponemon Institute, sponsorizzato da IBM Security, "The Cyber Resilient Organization", aprile 2019. ibm.com/account/reg/us-en/signup?formid=urx-37792.

7 IBM Security, "2019 Cost of a Data Breach Report", 2019. ibm.com/security/data-breach.

Integrazione degli strumenti, dei sistemi e dei processi di sicurezza attraverso l'automazione

Unificare persone, processi e strumenti con una piattaforma flessibile e coerente

Una piattaforma di automazione consente l'integrazione fra team, strumenti e processi di sicurezza. Una piattaforma flessibile e interoperabile consente di:

- Connettere sistemi, strumenti e team di sicurezza.
- Ottenere informazioni dai sistemi e inoltrarle rapidamente a sedi e sistemi predefiniti, senza richiedere alcun intervento manuale.
- Modificare e propagare le configurazioni velocemente tramite interfacce centralizzate.
- Creare, gestire e consultare i contenuti di automazione personalizzati correlati agli strumenti e ai processi di sicurezza in uso.
- Attivare interventi automatici tramite più strumenti di sicurezza, al rilevamento di una minaccia.

Utilizzare una piattaforma di automazione e un linguaggio coerenti in tutta l'azienda consente inoltre di migliorare la comunicazione e la collaborazione. Automatizzando tutte le soluzioni di sicurezza con lo stesso linguaggio, analisti e operatori possono eseguire in modo molto più rapido una serie di azioni su i diversi prodotti, massimizzando l'efficienza complessiva del team di sicurezza. Inoltre, utilizzando un framework e un linguaggio comuni, i team IT e di sicurezza possono condividere molto più facilmente progetti, processi e idee, sia internamente che con il resto dell'organizzazione.

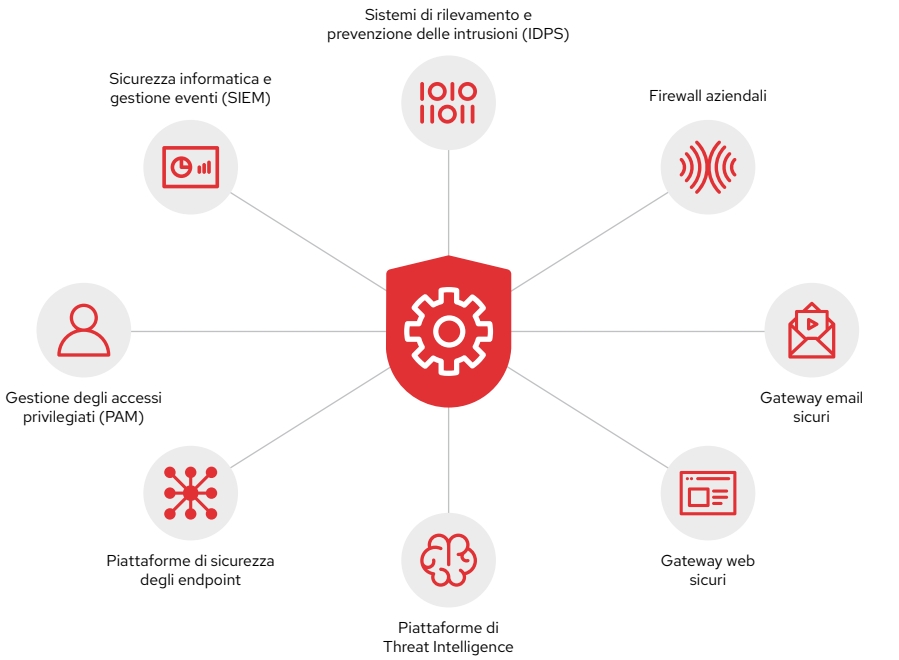


Figura 1. Una piattaforma di automazione consente di connettere sistemi, strumenti e team di sicurezza.

Successo dell'automazione = persone + processi + piattaforma

Per massimizzare il valore dell'automazione non basta uno strumento, ma occorre un approccio che tenga conto delle persone, dei processi e della piattaforma.

- Le **persone** costituiscono l'elemento chiave di tutte le iniziative aziendali. La partecipazione all'interno dei team e fra team diversi consente di condividere idee e collaborare più efficacemente.
- I **processi** consentono ai progetti di progredire da una fase a quella successiva, dall'inizio alla fine. Per un'automazione efficace sono necessari processi chiari e documentati.
- Una **piattaforma** di automazione offre tutte le funzionalità necessarie per creare, eseguire e gestire i tuoi asset di automazione. Diversamente dai semplici strumenti di automazione, offre una base uniforme per creare, distribuire e condividere contenuti e competenze coerenti su larga scala.

Leggi l'ebook

Il percorso di automazione della sicurezza

Adottare l'automazione in tutte le aree dell'organizzazione non è un'operazione immediata e non richiede l'automazione di tutte le funzioni. L'automazione della sicurezza è un percorso, che ogni azienda può iniziare e interrompere a seconda delle proprie esigenze. Tali esigenze determinano anche le scelte specifiche dell'azienda. In ogni caso, qualunque sia il percorso scelto, anche un livello minimo di automazione della sicurezza può garantire diversi vantaggi.

Valuta il livello di maturità della tua azienda nel percorso di automazione della sicurezza

In generale, il percorso di automazione della sicurezza può essere suddiviso in tre fasi. Determinando la fase attuale dell'azienda, è possibile adottare gli strumenti e i processi più appropriati per aumentare l'efficacia del percorso di automazione.

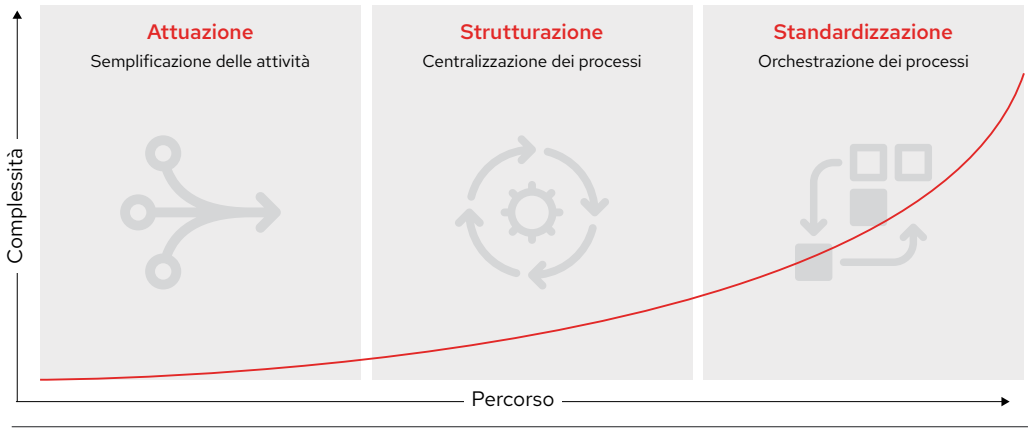


Figura 2. *Fasi della maturità nel percorso di automazione della sicurezza*

Fase 1: Attuazione

L'obiettivo, in questa fase, è risparmiare tempo automatizzando le operazioni finalizzate a garantire la sicurezza. Per raggiungere questo obiettivo, questa fase prevede la standardizzazione delle azioni di sicurezza fra dispositivi e tecnologie simili, oltre alla semplificazione delle attività manuali eseguite in prodotti di fornitori diversi.

Fase 2: Strutturazione

Questa fase ha lo scopo di migliorare i processi e l'efficienza, attraverso l'adozione di una serie di strumenti e servizi utili a garantire la sicurezza. Ad esempio, questa fase include l'integrazione dei processi di sicurezza nei flussi di lavoro più critici e la centralizzazione dei processi che consentono di risolvere i problemi legati alla sicurezza.

Fase 3: Standardizzazione

Questa fase ha lo scopo di massimizzare la collaborazione e integrare la sicurezza in tutti i livelli dell'organizzazione. Gli obiettivi più comuni includono la creazione di flussi di lavoro automatizzati e programmatici che coprono tutti gli aspetti della sicurezza e della relativa integrazione con le tecnologie IT.

Leggi l'articolo del blog

Definisci il tuo percorso di automazione della sicurezza

Scenari di utilizzo più comuni per l'automazione della sicurezza

Ciascuno di questi scenari di utilizzo può costituire un punto di partenza per il tuo percorso di automazione della sicurezza. L'importante è iniziare da un progetto piccolo e semplice, da sviluppare nel tempo.

Informazioni di supporto per le analisi

Per analizzare gli avvisi e gli incidenti di sicurezza è necessario raccogliere informazioni da diversi sistemi di sicurezza, allo scopo di determinare se si è verificato un problema. Solitamente è possibile reperire tali informazioni attraverso interfacce utente, email e chiamate telefoniche. Si tratta di un processo inefficiente che può ritardare gli interventi finalizzati a contrastare le minacce, esporre l'azienda ad ulteriori attacchi e incrementare i costi derivanti dalle violazioni. L'automazione offre gli strumenti necessari per ottenere informazioni da tutti i sistemi utilizzati, e consente di migliorare le attività di triage effettuate tramite i sistemi di sicurezza informatica e gestione degli eventi (SIEM, Security Information and Event Management) al fine di accelerare la valutazione di avvisi e incidenti, e la relativa risposta.

Ricerca delle minacce

La ricerca delle minacce consiste nell'identificazione e nell'analisi delle potenziali minacce alla sicurezza, con modalità proattive. Come avviene per l'analisi degli incidenti, il personale raccoglie e scambia informazioni manualmente utilizzando diversi sistemi. L'automazione consente di personalizzare e semplificare gli avvisi, la ricerca delle correlazioni e l'elaborazione delle firme, per accelerare l'analisi delle potenziali minacce. È inoltre possibile creare e aggiornare automaticamente le query di correlazione nei sistemi SIEM e le regole dei sistemi di rilevamento delle intrusioni (IDS, Intrusion Detection System) per migliorare l'identificazione delle minacce. Questo consente di aggiornare gli strumenti di sicurezza dell'azienda in modo più frequente ed efficace.

Risposta agli incidenti

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, che rallentano l'intervento e aumentano la durata dell'esposizione alla minaccia. L'automazione permette di reagire più velocemente, codificando le azioni 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.

Il ruolo essenziale dell'integrazione

Gli approcci unificati all'automazione richiedono l'integrazione fra la piattaforma di automazione e le tecnologie di sicurezza. Le integrazioni essenziali includono:

- **Firewall,** che controllano il flusso del traffico tra le reti, proteggendo le applicazioni esposte a Internet. L'automazione consente di accelerare le modifiche alla configurazione di policy e log.
- **I sistemi di rilevamento e prevenzione delle intrusioni (IDPS, Intrusion Detection and Prevention System)** consentono di monitorare il traffico di rete al fine di individuare attività sospette, segnalando le minacce e bloccando gli attacchi. L'automazione può semplificare la gestione di regole e log.
- **I sistemi di sicurezza informatica e gestione degli eventi (SIEM, Security Information and Event Management)** raccolgono e analizzano gli eventi di sicurezza, per semplificare il rilevamento delle minacce e la relativa risposta. L'automazione offre un accesso programmatico alle sorgenti di dati.
- **I sistemi di gestione degli accessi privilegiati (PAM, Privileged Access Management)** consentono di monitorare e gestire gli account e gli accessi privilegiati. L'automazione semplifica la gestione delle credenziali.
- **I sistemi di protezione degli endpoint** consentono di monitorare e gestire i dispositivi per aumentarne la sicurezza. L'automazione può semplificare le normali attività di gestione degli endpoint.

Scopri di più

Semplifica il tuo centro operativo di sicurezza con Red Hat Ansible Automation Platform

Sul mercato sono disponibili moltissime soluzioni di automazione, ma non tutte offrono le funzionalità necessarie per automatizzare efficacemente la sicurezza. La piattaforma di automazione scelta deve offrire:

- **Un linguaggio di automazione universale e accessibile.** Un linguaggio facile da comprendere e scrivere consente ai membri dei team dedicati alla sicurezza con competenze diverse di documentare e condividere le informazioni.
- **Un approccio aperto e obiettivo.** Per essere efficace, una piattaforma di automazione deve essere in grado di interagire con l'intera infrastruttura di sicurezza e tutto l'ecosistema di fornitori.
- **Un'architettura modulare e scalabile.** Una piattaforma modulare consente il deployment graduale dell'automazione. La scalabilità consente di integrare ulteriori strumenti di sicurezza di altri fornitori, a seconda delle esigenze.

Consenti ai tuoi team di evolversi con Red Hat

La soluzione **Red Hat® Ansible® Automation Platform** offre una base solida per creare e gestire i servizi di automazione su vasta scala, fornendo tutti gli strumenti e le funzionalità necessari per implementare l'automazione della sicurezza. La piattaforma offre un linguaggio semplice, a cui si aggiungono un ambiente di esecuzione componibile e funzionalità di condivisione e collaborazione incentrate sulla sicurezza. La base open source consente di connettere e automatizzare quasi tutti gli elementi dell'infrastruttura IT e di sicurezza, offrendo una piattaforma comune che supporta la collaborazione e la condivisione a tutti i livelli dell'azienda. Red Hat Ansible Automation Platform ha dimostrato di offrire vantaggi concreti anche in altre aree, tra cui operazioni IT, di rete e DevOps.

La piattaforma comprende un insieme supportato di **raccolte Ansible incentrate sulla sicurezza**, che includono moduli, ruoli e playbook. È possibile coordinare le attività di varie tipologie di soluzioni e unificare più efficacemente le operazioni di sicurezza e la risposta alle minacce attraverso:

- Flussi integrati e playbook per consentire il riutilizzo modulare.
- Log consolidati e centralizzati.
- Supporto per i servizi delle directory locali e il controllo degli accessi.
- Integrazione con app esterne tramite API (Application Programming Interface) RESTful.

Red Hat Ansible Automation Platform offre anche strumenti e funzionalità che consentono di ottimizzare l'automazione. **Automation Analytics** fornisce informazioni dettagliate sull'uso dell'automazione all'interno dell'azienda. **Automation Hub** consente ai membri dei team di accedere a contenuti certificati sull'automazione, tramite un repository centralizzato. Inoltre, le **raccolte di contenuti** semplificano la gestione, la distribuzione e l'utilizzo degli asset di automazione.

Fatti aiutare dagli esperti

Red Hat può aiutarti ad accelerare l'automazione.

- **Red Hat Services Program: Automation Adoption** propone un framework per l'adozione e la gestione dell'automazione nell'intera azienda.
- **Red Hat Training and Certification** offre formazione pratica e certificazioni per aiutarti a utilizzare l'automazione in modo più efficace.
- **Red Hat Support** collabora con la tua azienda per consentire un utilizzo efficace delle tecnologie. Il nostro pluripremiato supporto online[8] ti permette di accedere a best practice, documentazione, aggiornamenti, patch e avvisi di sicurezza. Contattando un ingegnere del supporto tecnico o un Technical Account Manager potrai risolvere problemi e ottenere indicazioni specifiche.
- Le **raccolte di contenuti per i partner certificati** consentono di automatizzare velocemente componenti hardware e software di una vasta gamma di fornitori. Questi affidabili contenuti di automazione pronti all'uso sono accessibili tramite Automation Hub e sono supportati da Red Hat e dai partner.

8 Red Hat Customer Portal, premi e riconoscimenti: **access.redhat.com/recognition**.

Vantaggi dell'automazione:

il valore di Red Hat Ansible Automation Platform

Red Hat Ansible Automation Platform consente di automatizzare il centro operativo di sicurezza in modo più semplice ed efficiente. Gli studi degli analisti sulle aziende che utilizzano Red Hat Ansible Automation Platform dimostrano che questa soluzione offre un valore di business misurabile. Chiedendo a vari decision maker di raccontare la loro esperienza con Red Hat Ansible Automation Platform, **IDC** ha riscontrato che l'automazione ha consentito a tutte le aziende intervistate di ottenere notevoli vantaggi a livello di produttività, agilità e operazioni.

aumento dei livelli di efficienza e produttività dei team di sicurezza IT[9]

aumento dell'efficienza nel contenimento degli incidenti[9]

aumento dell'efficienza nell'applicazione delle patch di sicurezza[9]

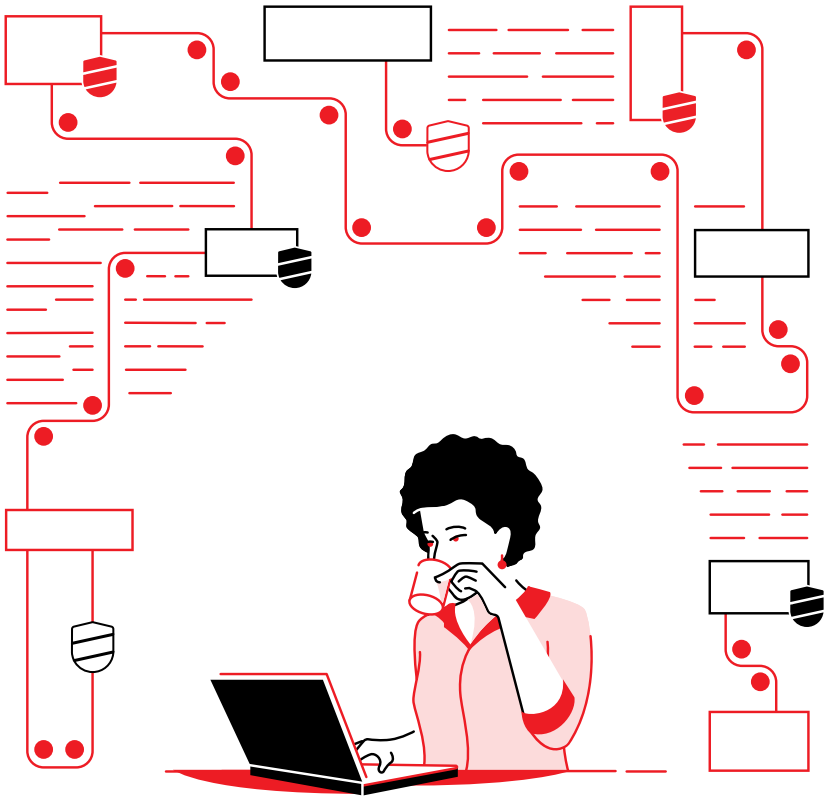
"Red Hat Ansible [Automation Platform] permette una collaborazione straordinaria fra i team IT. I team responsabili di server, sicurezza, rete e database possono tutti svolgere il loro lavoro separatamente e utilizzare Red Hat Ansible Automation per creare playbook personalizzati."[9]

Leggi il resoconto analitico

9 *Whitepaper di IDC, sponsorizzato da Red Hat. "Red Hat Ansible Automation Improves IT Agility and Time to Market", giugno 2019.* **redhat.com/it/resources/business-value-red-hat-ansible-automation-analyst-paper**.

Scopri come semplificare il tuo centro operativo di sicurezza

L'automazione può aiutarti a identificare e gestire un numero sempre crescente di minacce alla sicurezza, più rapidamente e su vasta scala. Red Hat ti aiuta a proteggere l'azienda connettendo team, strumenti e processi di sicurezza con una piattaforma di automazione coerente e collaborativa.



Scopri come automatizzare la sicurezza con Red Hat Ansible Automation Platform: **red.ht/automate-security**

F24343_0720_KVM

Red Hat