Red Hat

Rafforzare la sicurezza con l'automazione

Storie di successo dei clienti Red Hat

Sommario

Introduzione

L'automazione sta trasformando la sicurezza

Riuscire a integrate i team e le soluzioni di sicurezza dell'IT in un ambiente in continua evoluzione è oggi un problema che interessa qualunque tipo di organizzazione. Ogni approccio alla sicurezza è unico, esistono però delle strategie che si possono imparare e adattare per proteggere i dati, le applicazioni, i sistemi IT, le reti e i dispositivi da attività malevole o indesiderate.

Per illustrare tali strategie, abbiamo raccolto in questo ebook cinque storie di successo selezionate fra gli utenti di Red Hat® Ansible® Automation Platform che utilizzano l'automazione per favorire l'integrazione e la scalabilità delle loro soluzioni di sicurezza e in questo modo rilevare e rispondere alle minacce nell'intera organizzazione in modo coordinato e unificato.

Perché l'automazione rafforza la sicurezza?

La maggior parte delle organizzazioni dispone di un team di sicurezza competente che sa cosa occorre fare per garantire la sicurezza. Il problema è che configurare migliaia di sistemi e applicazioni manualmente per proteggerli dagli attacchi esterni è un compito che richiede più tempo e risorse specializzate di quanto sia sostenibile.

Da questo punto di vista l'automazione offre un valido contributo perché permette di applicare e mantenere standard di sicurezza che si adattano per soddisfare i requisiti di sicurezza interni ed esterni. I risultati più evidenti dell'automazione sono l'accelerazione dei tempi di risposta e la riduzione del livello di vulnerabilità.

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

Ansible Automation Platform consente di automatizzare e integrare le soluzioni di sicurezza e permette così di rilevare e rispondere alle minacce in tutta l'azienda in modo coordinato e unificato grazie a una raccolta idonea di moduli, ruoli e playbook.

Cosa prevede un approccio alla sicurezza unificato?

Le soluzioni di sicurezza devono evolversi costantemente per stare sempre un passo avanti alle minacce. Ecco alcuni aspetti chiave da considerare:

Informazioni di supporto per le analisi

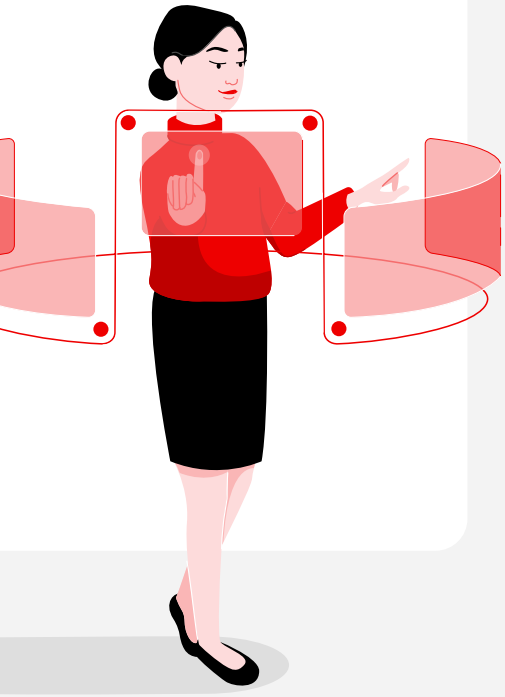
Raccogli i dati di firewall, sistemi di rilevamento delle intrusioni (IDS) e altri sistemi di sicurezza per supportare le attività di triage delle soluzioni SIEM (Security Information and Event Management Systems).

Rilevamento delle minacce

Ottimizza automaticamente il livello di registrazione e crea nuove regole IDS e nuovi criteri firewall per individuare le minacce più rapidamente.

Risposta agli incidenti

Accelera la correzione dei problemi tramite la creazione di denylist per gli indirizzi IP o i domini pericolosi, di allowlist per i flussi di traffico legittimi e l'isolamento dei carichi di lavoro sospetti.



Perché automatizzare la sicurezza con Ansible?

La sicurezza è una responsabilità condivisa. Ansible è uno strumento agentless con enormi potenzialità che rende l'automazione accessibile a tutta l'azienda, dai team operativi, di sviluppo e di progettazione della rete fino a quelli di sicurezza, perché prevede l'utilizzo di un linguaggio leggibile in chiaro. In questo modo le organizzazioni possono sfruttare a pieno i vantaggi dell'automazione con cui riescono a:

- Aumentare la produttività. Ansible utilizza un linguaggio semplice e leggibile in chiaro. Questo significa che non occorrono competenze specialistiche di programmazione o gestione per controllare che le attività siano eseguite nell'ordine corretto.
- Gestire tutta l'infrastruttura IT. Ansible consente di raccogliere e verificare le informazioni, oltre a semplificare la gestione delle configurazioni e l'orchestrazione dei flussi di lavoro.
- Aumentare l'efficienza e la sicurezza. Con un'architettura agentless è possibile accelerare il deployment delle soluzioni senza doversi preoccupare dell'esecuzione o dell'aggiornamento degli agenti.

Le storie di successo riportate di seguito illustrano le potenzialità e la scalabilità dell'automazione applicata alla sicurezza e mostrano come una piattaforma di automazione unificata come Ansible Automation Platform possa davvero aiutare le aziende a rafforzare la sicurezza.

1

EMORY UNIVERSITY

La Emory University contiene le minacce alla utility sudo con Red Hat Ansible Automation Platform

> *Nessuno credeva che saremmo riusciti ad applicare le patch ai server Linux ogni 30 giorni, ma con Red Hat Ansible Automation Platform ce l'abbiamo fatta.*
>
> Steve Siegelman, Manager of Systems Engineering, Office of Information Technology, Emory University

La Emory University di Atlanta, Georgia, conta oltre 15.000 studenti nei campus dell'area metropolitana della città. Non sorprende che l'ambiente digitale di un'università come questa, che intrattiene rapporti di ricerca con istituzioni di tutto il mondo ed è a capo della gestione del più grande sistema sanitario della Georgia, sia oggetto di attacchi informatici mirati a ottenere l'accesso a informazioni riservate.

La preoccupazione principale è che, una volta entrati nel sistema attraverso un punto vulnerabile, gli hacker possano muoversi indisturbati in tutta la rete, arrivare alle proprietà intellettuali e uscire dal sistema senza lasciare traccia. L'università dispone infatti di un Office of Information Technology (OIT) che si occupa di aggiornare i sistemi e di garantire la sicurezza della rete e dei dati di studenti, personale tecnico, docenti e ricercatori contro accessi non autorizzati o violazioni. Ciononostante si è creata non poca agitazione quando nel gennaio 2021 il team di Red Hat ha avvertito l'OIT della presenza di una vulnerabilità nei sistemi Red Hat Enterprise Linux® dell'istituzione che coinvolgeva la utility sudo del sistema operativo.

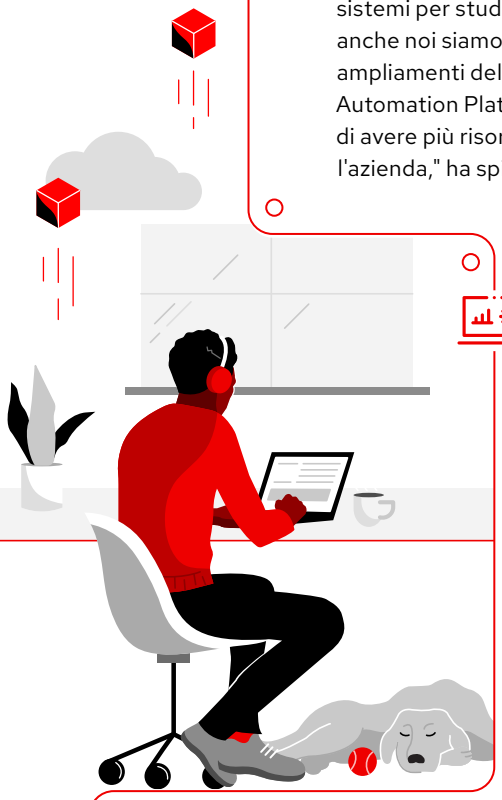
L'automazione di Ansible accelera la correzione dei rischi di sicurezza

Applicazione di patch in poche ore

Con più di 500 server che utilizzano Red Hat Enterprise Linux da monitorare, l'OIT della Emory University sapeva che l'installazione manuale delle patch sarebbe stata un compito troppo gravoso e che avrebbe messo in pericolo la sicurezza dell'infrastruttura. La soluzione è stata utilizzare un Ansible Playbook per applicare le patch automaticamente a tutti i server. Così facendo l'attività di correzione che altrimenti avrebbe richiesto fino a due settimane è stata completata in appena quattro ore.

Più risorse da dedicare ai progetti strategici

La Emory University ha adottato Ansible Automation Platform prima per i suoi sistemi finanziari e poi ne ha esteso l'utilizzo anche ai sistemi per studenti e risorse umane. "Come succede in molte realtà, anche noi siamo chiamati a fare sempre di più senza però adeguati ampliamenti del personale. Disporre di uno strumento come Ansible Automation Platform che si occupa delle attività ripetitive permette di avere più risorse a disposizione da dedicare a progetti strategici per l'azienda," ha spiegato Siegelman.



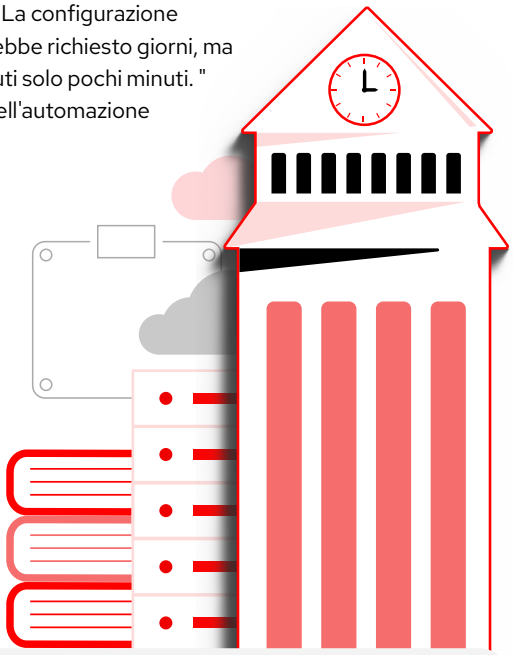
Lo staff IT si è potuto concentrare sulla sfide poste dal COVID-19

Un altro esempio della flessibilità di Ansible Automation Platform si è visto nel marzo 2020 quando la Emory University, come quasi tutte le università e le aziende, è stata costretta a chiudere e a far proseguire le sue attività da remoto.

In quel caso l'OIT si è trovato a dover distribuire rapidamente server di database per gestire il monitoraggio dei dipendenti essenziali e concedere loro l'autorizzazione a restare nel campus. I dipendenti dovevano completare dei questionari da inserire nel sistema. La configurazione manuale di questo genere di attività sui server avrebbe richiesto giorni, ma grazie ad Ansible Automation Platform ci sono voluti solo pochi minuti. " È stata la dimostrazione chiara delle potenzialità dell'automazione per il back end," ha detto Siegelman.

Innovazione della sicurezza al di là del campus con l'automazione

L'automazione giocherà un ruolo chiave anche nel futuro della Emory University che ha avviato un percorso di transizione al cloud. "Disponiamo di alcuni sistemi tradizioni che sono un insieme di build nuove e più datate e stiamo investendo grandi risorse ed energie sulla piattaforma AWS," ha spiegato Siegelman. "Ansible Automation Platform ci permette di utilizzare gli stessi processi ripetibili in tutti i sistemi anche se diversi fra loro. Non importa se la piattaforma è on premise o nel cloud, tutto funziona a dovere."



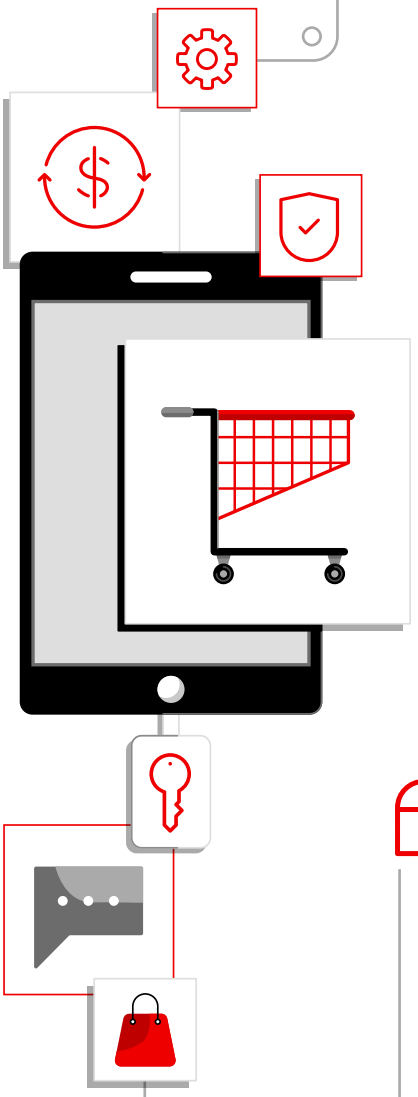
Scarica
la storia di successo della Emory University

2

Schwarz Group automatizza l'IT con Red Hat Ansible Automation Platform

Lo Schwarz Group, quarta società di retail al mondo, conta oltre 12.500 punti vendita in 33 Paesi. Il gruppo desidera estendere la propria presenza internazionale, ma per riuscirci deve trovare il giusto equilibrio tra la gestione coerente dei punti vendita, il mantenimento della flessibilità necessaria per soddisfare le esigenze locali, l'agilità per aprire nuovi punti vendita soprattutto nei nuovi mercati e la capacità di contenere i rischi.

Per uniformare l'amministrazione dei punti vendita e mantenere un livello di flessibilità tale da adattarsi alle esigenze locali, Schwarz ha scelto di eseguire la migrazione da Puppet a Red Hat Ansible Automation Platform. Con una base operativa coerente il gruppo può sfruttare le capacità self service per accelerare il deployment di servizi digitali innovativi e rimanere competitiva senza mettere a rischio la sicurezza.



La coerenza è la chiave per garantire la sicurezza di migliaia di punti vendita nel mondo

Il team IT di Schwarz comprende più di 3500 ingegneri che lavorano per supportare oltre 1000 sistemi SAP e 28PB di storage in hosting su datacenter. Ogni negozio del gruppo esegue uno Storeserver, un sistema operativo centrale installato dal team IT locale, che controlla tutta una serie di funzioni di quel punto vendita come ad esempio i sistemi di cassa, i sistemi di videosorveglianza a circuito chiuso, ma anche i programmi di riciclo e di raccolta punti.

Per ottimizzare l'autorizzazione e la gestione degli utenti, il team IT di Schwarz puntava a introdurre capacità self service efficienti e controllate con cui velocizzare i processi di deployment. Ha scelto quindi di adottare Ansible Automation Platform.

> *Considerata la complessità e la lunghezza dei processi, la versione community non era adatta alle nostre esigenze. L'automazione è un aspetto essenziale per la nostra attività, e l'offerta di un supporto di livello enterprise è stata una delle ragioni chiave che ci hanno portato a scegliere la soluzione di Red Hat.*
>
> Felix Kuehner, Head of Storeserver, Core Infrastructure Services, Schwarz IT

Durante un workshop di due giorni, il team IT di Schwarz ha potuto lavorare fianco a fianco con gli esperti di Red Hat per esaminare l'architettura e definire procedure consigliate per la nuova soluzione di automazione.

Oggi per gestire i server dei suoi punti vendita, il gruppo esegue quotidianamente oltre 5000 processi di automazione con Ansible Automation Platform.

Gestione dei rischi migliorata con il controllo degli accessi basato sui ruoli

Grazie ad Ansible Automation Platform, il team IT di Schwarz è in grado di controllare più agevolmente gli accessi al sistema e ha a disposizione il giusto livello di capacità self service per accelerare le attività di sviluppo. Con il controllo degli accessi basato sui ruoli, i team che si occupano delle applicazioni possono automatizzare i deployment come utenti standard, senza dover richiedere l'accesso root per i sistemi aziendali principali. "Questa funzionalità fornisce un elevato livello di coerenza e permette ai nostri dipendenti di lavorare in modo proattivo sui progetti nuovi e su quelli esistenti," ha affermato Kuehner.

Dopo questo primo successo con Ansible Automation Platform, il team IT di Schwarz intende continuare a sondare le potenzialità di Ansible per migliorare ancora di più la coerenza e la reattività dei suoi punti vendita.

> *Abbiamo apprezzato il lavoro fatto con Red Hat e ci auguriamo di continuare a utilizzare Ansible per modernizzare e ottimizzare la nostra attività.*
>
> Felix Kuehner, Head of Storeserver, Core Infrastructure Services, Schwarz IT

Scarica
la storia di successo di Schwarz

Agile Defense migliora la conformità alle normative di sicurezza con Red Hat Ansible Automation Platform

3

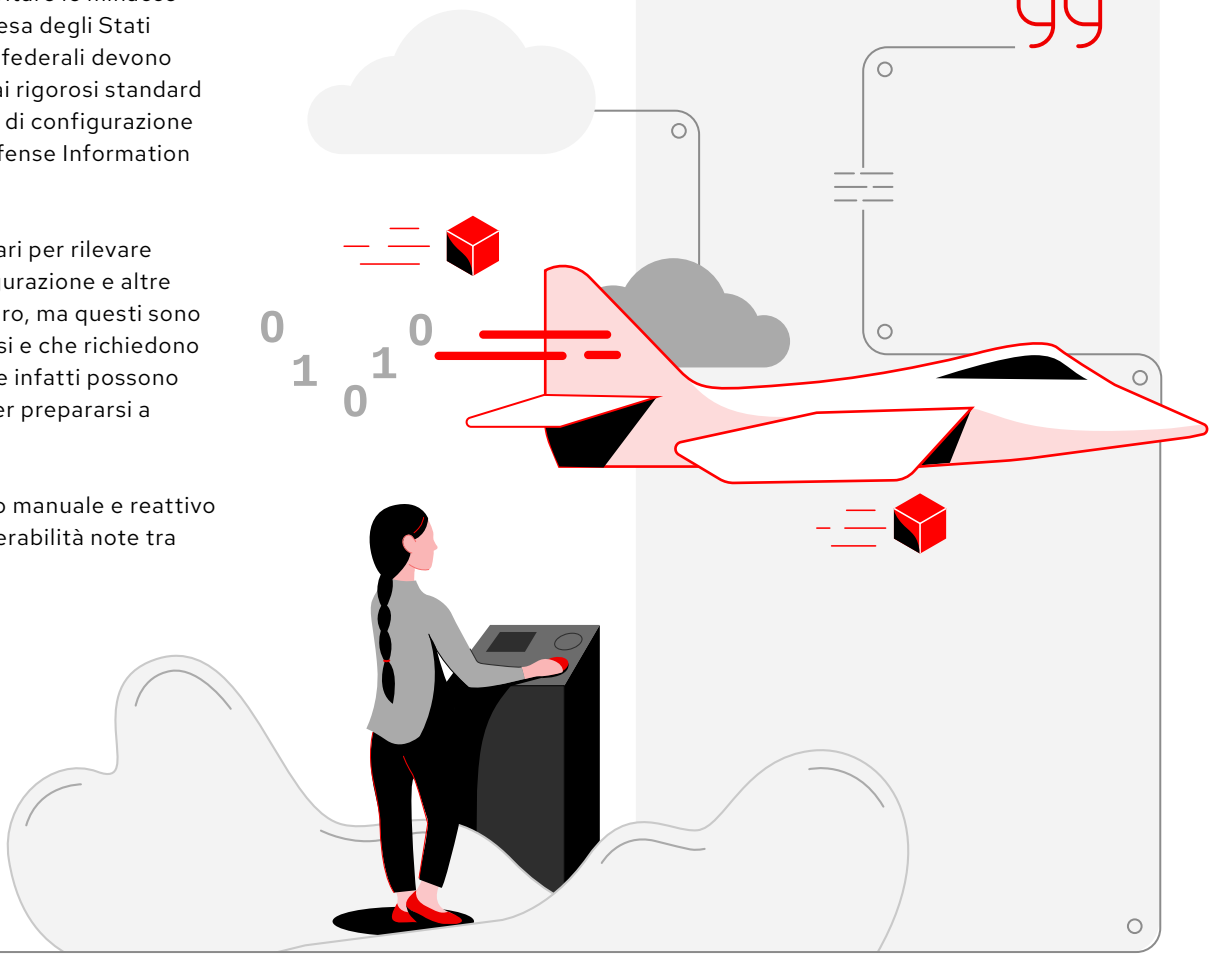
Agile Defense, con sede a Reston in Virginia, è un'azienda leader nel settore dei servizi informatici. Per un'organizzazione del suo calibro, che vanta tra i suoi clienti numerose agenzie civili collegate al Governo degli Stati Uniti e diversi reparti del Dipartimento della Difesa degli Stati Uniti, la sicurezza dell'IT è una priorità.

Impedire agli hacker di accedere ai sistemi e all'infrastruttura aziendale non è mai stato tanto importante. Tra le cause più frequenti delle violazioni spiccano gli errori di configurazione. Per evitare le minacce il Dipartimento della Difesa degli Stati Uniti (DoD) e le agenzie federali devono garantire la conformità ai rigorosi standard informatici, di sicurezza, di configurazione e di conformità della Defense Information Systems Agency (DISA).

Sottoporsi a audit regolari per rilevare eventuali errori di configurazione e altre criticità fa parte del lavoro, ma questi sono controlli ripetitivi, costosi e che richiedono molte risorse. Le agenzie infatti possono impiegare anche mesi per prepararsi a un'ispezione.

La scelta di un approccio manuale e reattivo esponeva i clienti a vulnerabilità note tra un'ispezione e l'altra.

> ***Prima di un'ispezione i nostri clienti praticamente interrompevano le attività di produzione per poter preparare la documentazione.***
>
> Shawn Draper, Solutions Engineer, Agile Defense



L'automazione aiuta a limitare l'impatto degli audit

Gli errori di configurazione e gli audit sono due aspetti critici per molti dei clienti di Agile Defense. L'azienda, che punta a fornire servizi informatici all'avanguardia, ha quindi collaborato con Red Hat alla creazione di uno strumento di configurazione, correzione e reportistica basato su STIG (Security Technical Implementation Guide). Questa soluzione di automazione STIG è in grado di eseguire controlli ad hoc sui sistemi, correggere gli errori di configurazione se richiesto e generare report sullo stato dei dispositivi. Altrimenti nota come lo strumento Compliance-as-a-Service (CPaaS) di Agile Defense, la soluzione di automazione STIG utilizza Red Hat Ansible Automation Platform per via delle sue funzionalità di automazione scalabili e flessibili.

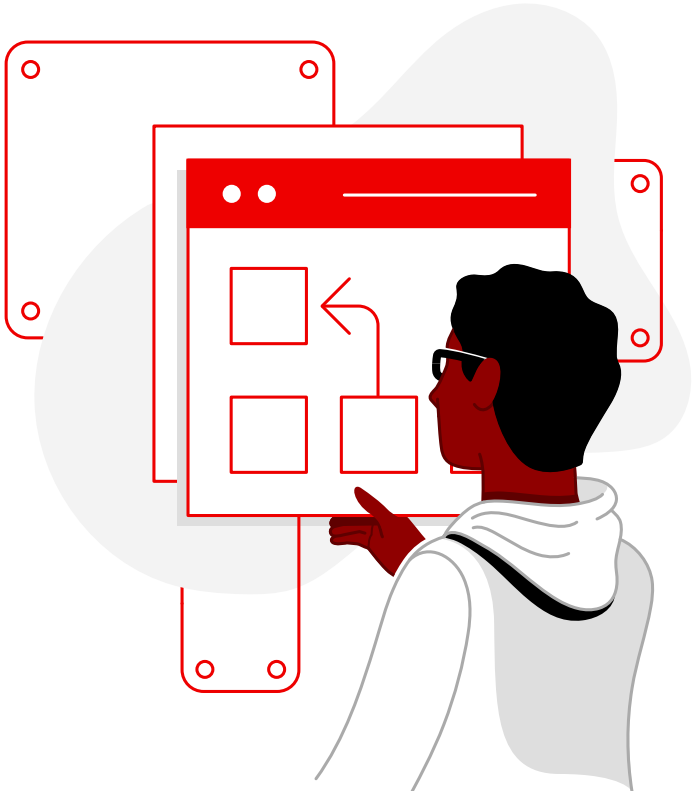
Inoltre, Red Hat, che comprende bene l'importanza di creare standard per ogni dispositivo, sistema operativo e versione dei software, ha collaborato con DISA alla realizzazione di uno STIG per Red Hat Enterprise Linux.

> ***Per risolvere il problema abbiamo scelto Red Hat Ansible Automation Platform perché è compatibile con la maggior parte dei sistemi.***
>
> Shawn Draper, Solutions Engineer, Agile Defense

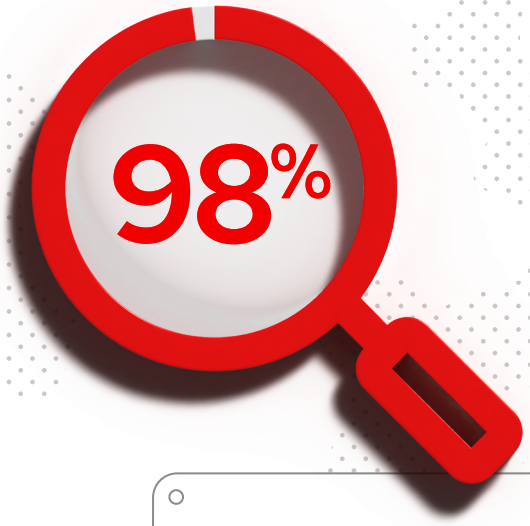
I vantaggi degli Ansible Playbook per la sicurezza

La soluzione CPaaS utilizza le funzionalità di automazione della gestione della configurazione fornite da Red Hat Ansible Automation Platform per controllare la presenza di vulnerabilità aperte. "Red Hat Ansible Automation Platform si collega ai dispositivi ed esegue i comandi definiti in un Ansible Playbook," ha spiegato Draper.

Una volta rilevati gli errori di configurazione in maniera automatica, la soluzione CPaaS è anche in grado applicare le dovute correzioni in base ai comandi specifici definiti negli Ansible Playbook. Agile Defense ha creato un'ampia gamma di playbook personalizzati adatti a testare diverse tipologie di dispositivi, come ad esempio le piattaforme Red Hat, i dispositivi Windows, gli hypervisor VMware, i router e gli switch Cisco e i firewall.



Riduzione del tempo dedicato agli audit del



La soluzione CPaaS genera anche tutta la documentazione necessaria. Nello specifico la soluzione utilizza Ansible Automation Platform per generare un file di controllo XML (consultabile nello STIG Viewer di DISA) per ogni dispositivo della rete e per ogni vulnerabilità identificata, che l'azienda potrà presentare all'ispettore che condurrà l'audit. Questi documenti contengono informazioni utili sullo stato dei dispositivi e dimostrano se una determinata configurazione di sicurezza è stata implementata o meno. Ansible Automation Platform permette anche di estendere la capacità di CPaaS alla gestione dei flussi di lavoro e degli inventari, alla pianificazione degli audit e al controllo degli accessi basato sui ruoli. Inoltre, la soluzione CPaaS contribuisce a migliorare la coerenza fra i diversi dispositivi aziendali.

> ***L'automazione assicura che un'azione venga eseguita sempre allo stesso modo.***
>
> Shawn Draper

L'approccio proattivo al monitoraggio della sicurezza offerto dalla soluzione CPaaS è essenziale per prevenire gli attacchi informatici. Le attività di monitoraggio dei sistemi sono da sempre un punto critico per le organizzazioni perché richiedono non solo notevoli risorse ma anche l'installazione di software supplementari sui dispositivi da esaminare. Sfruttando le funzionalità di Ansible Automation Platform invece la soluzione CPaaS di Agile Defense è in grado di rilevare la presenza di vulnerabilità aperte e permette di ridurre del 98% il tempo dedicato agli audit.

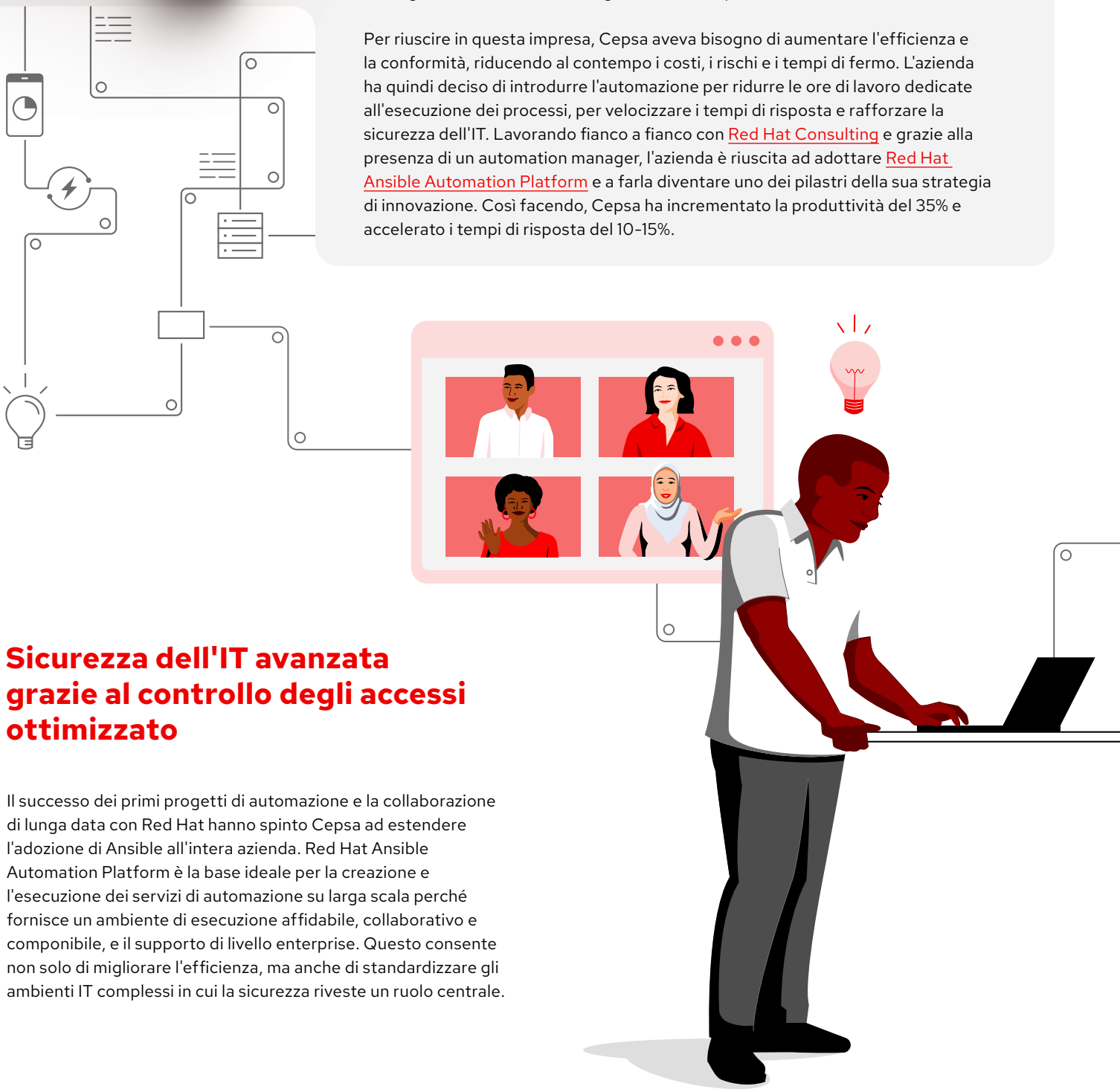
Scarica
la storia di successo di Agile Defense

4

Cepsa ottiene più efficienza con Red Hat Ansible Automation Platform

Cepsa, un'azienda leader nel settore energetico e chimico, lavora per la riduzione delle emissioni di carbonio in tutto il mondo. Nel 2022 l'azienda ha presentato la sua strategia per diventare una realtà di primo piano nell'ambito di mobilità sostenibile, biocarburanti e idrogeno verde, che prevedeva un focus specifico su Spagna e Portogallo e la transizione energetica come un punto di riferimento chiave.

Per riuscire in questa impresa, Cepsa aveva bisogno di aumentare l'efficienza e la conformità, riducendo al contempo i costi, i rischi e i tempi di fermo. L'azienda ha quindi deciso di introdurre l'automazione per ridurre le ore di lavoro dedicate all'esecuzione dei processi, per velocizzare i tempi di risposta e rafforzare la sicurezza dell'IT. Lavorando fianco a fianco con Red Hat Consulting e grazie alla presenza di un automation manager, l'azienda è riuscita ad adottare Red Hat Ansible Automation Platform e a farla diventare uno dei pilastri della sua strategia di innovazione. Così facendo, Cepsa ha incrementato la produttività del 35% e accelerato i tempi di risposta del 10-15%.



Sicurezza dell'IT avanzata grazie al controllo degli accessi ottimizzato

Il successo dei primi progetti di automazione e la collaborazione di lunga data con Red Hat hanno spinto Cepsa ad estendere l'adozione di Ansible all'intera azienda. Red Hat Ansible Automation Platform è la base ideale per la creazione e l'esecuzione dei servizi di automazione su larga scala perché fornisce un ambiente di esecuzione affidabile, collaborativo e componibile, e il supporto di livello enterprise. Questo consente non solo di migliorare l'efficienza, ma anche di standardizzare gli ambienti IT complessi in cui la sicurezza riveste un ruolo centrale.

La sintassi intuitiva degli Ansible Playbook ha permesso a Cepsa di definire agevolmente dei parametri di sicurezza per ogni aspetto del sistema, come ad esempio l'impostazione di regole firewall, il blocco di utenti o gruppi di utenti, e l'applicazione di criteri di sicurezza personalizzati. La standardizzazione dei processi ha aiutato Cepsa a contenere i rischi riducendo il numero di autorizzazioni aggiuntive per la gestione della sicurezza nei propri sistemi. Gli utenti sono oggi raggruppati per ruolo lavorativo e reparto, e ciò garantisce che ognuno disponga del livello di autorizzazione adeguato.

Così facendo, Cepsa ha incrementato la produttività del 35% e accelerato i tempi di risposta del 10-15%.

Un tecnico può accedere ad Ansible Automation Platform e riavviare il servizio senza bisogno di credenziali. Questo assicura che il processo venga eseguito come descritto nel codice predefinito.

Produttività
incrementata del **35%**

Tempi di risposta
ridotti del **10-15%**

L'automazione ha promosso un cambiamento culturale positivo per l'azienda che ci ha portati a migliorare la collaborazione fra i team. Continueremo a lavorare con il team di Red Hat per adottare procedure consigliate in tutta l'organizzazione e imparare dalla loro esperienza.

Francisco José Martín, Automation Manager,
Department of Exploitation and Operation, Cepsa

Una guida esperta verso una cultura orientata alla sicurezza

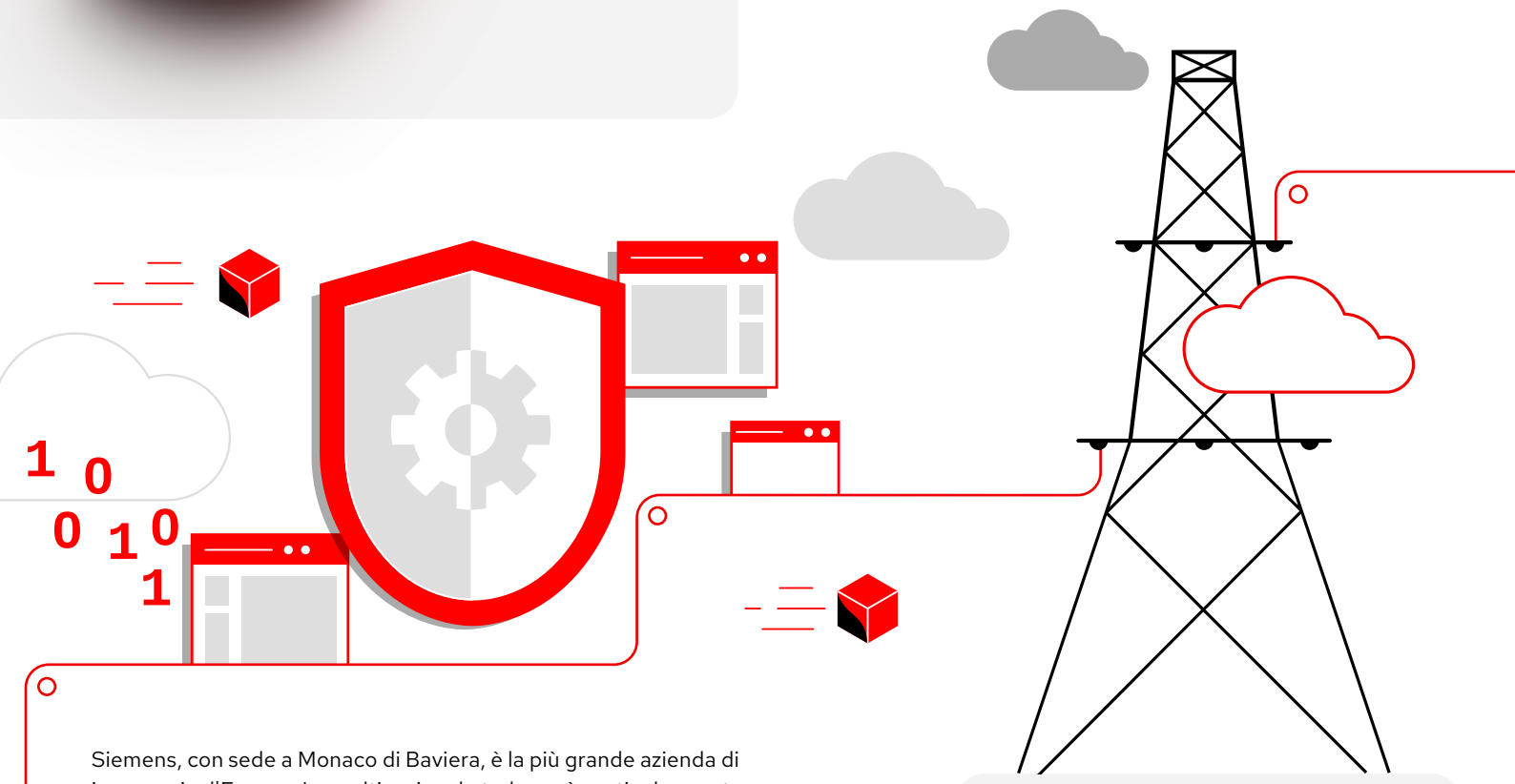
Red Hat Consulting ha aiutato Cepsa ad attuare le modifiche necessarie per ottenere il massimo dal nuovo approccio e dalle tecnologie per l'automazione. Lavorando fianco a fianco con gli esperti di Red Hat, il team di Cepsa ha potuto vedere in prima persona quali sono i vantaggi dell'approccio agile e del miglioramento continuo della qualità tramite pipeline di integrazione e distribuzione continue (CI/CD).

Scarica
la storia di successo
di Cepsa

5

SIEMENS

Siemens migliora la sicurezza delle comunicazioni con Red Hat Ansible Automation Platform



Siemens, con sede a Monaco di Baviera, è la più grande azienda di ingegneria d'Europa. La multinazionale tedesca è particolarmente attiva nelle aree dell'elettrificazione. Si occupa infatti di generazione, trasmissione e distribuzione dell'energia elettrica nonché di soluzioni per reti intelligenti e consumo efficiente dell'energia elettrica.

Data la natura delicata delle informazioni che processa, Siemens è sempre alla ricerca di tecnologie di sicurezza all'avanguardia. Per tutelare le informazioni confidenziali, i 295.000 dipendenti interni di Siemens e i 100.000 dei suoi partner utilizzano infrastrutture a chiave pubblica (PKI), che prevedono la verifica dei certificati e dell'identità delle chiavi pubbliche. L'infrastruttura PKI viene utilizzata anche per proteggere le comunicazioni associate all'Internet of Things (IoT); attualmente l'azienda gestisce due ambienti PKI per diversi scenari di utilizzo relativi alle applicazioni.

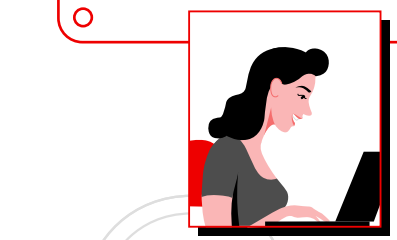
> ***Questo è importante perché adottare l'Infrastructure-as-Code di Red Hat Ansible Automation Platform non significa solo adottare un nuovo strumento. Richiede un cambio di mentalità da parte degli amministratore di sistema.***
>
> Rufus Buschart, Head of Public Key Infrastructure (PKI), Siemens

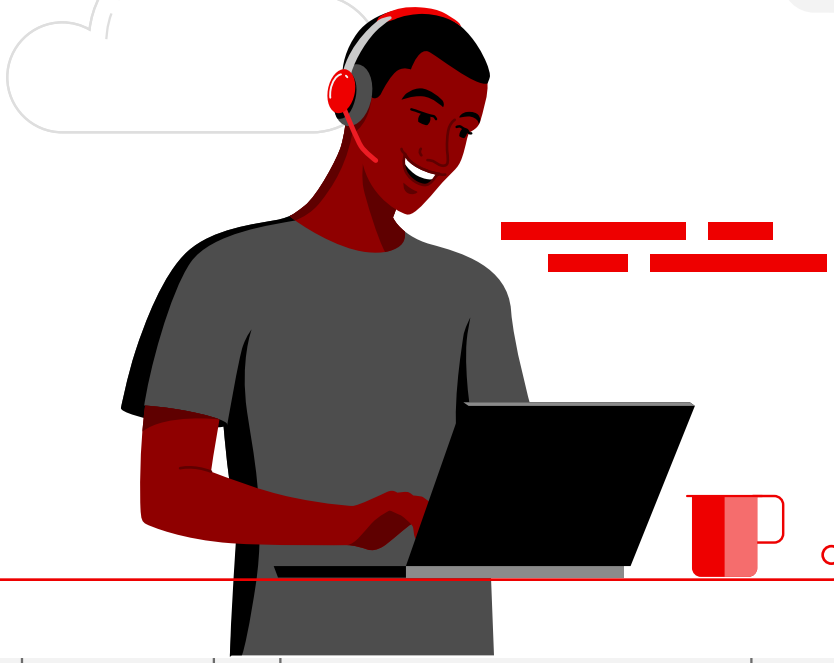
Qualunque cosa ci occorra, Red Hat è sempre disponibile. Abbiamo intenzione di lavorare con Red Hat per sviluppare una piattaforma di procedure consigliate per l'automazione con cui ottimizzare e migliorare la nostra azienda.

Rufus Buschart

Con l'aumento delle comunicazioni tra i team dei servizi, le attività di configurazione si fanno via via più gravose anche per i team PKI di Siemens. Per questo motivo l'azienda ha sostituito la soluzione di automazione in uso con Ansible Automation Platform.

Grazie ad Ansible Automation Platform, Siemens è stata in grado di automatizzare le attività amministrative, aumentare la qualità della configurazione e migliorare la sicurezza delle comunicazioni all'interno dell'organizzazione. Siemens ha inoltre potuto sfruttare l'esperienza di Red Hat e prevede di continuare a collaborare con lei a progetti di automazione dei processi di test al fine di sviluppare un modello comune per il deployment continuo.





Scarica
la storia di successo di Siemens

Con-clusioni

Ansible Automation Platform aiuta le organizzazioni a gestire i sistemi di sicurezza automatizzati per prevenire gli attacchi dannosi. Con centinaia di moduli che permettono ai team di sicurezza di automatizzare ogni aspetto dell'ambiente e dei processi IT, Ansible favorisce l'integrazione dei team aziendali perché operino in sinergia alla salvaguardia di perimetri di sicurezza complessi, crea un approccio alla sicurezza unificato e migliora il profilo di sicurezza.

Ansible Automation offre:

Flussi integrati e playbook per consentire il riutilizzo modulare.

I team di sicurezza possono configurare una sequenza di processi che condividono inventario, playbook o autorizzazioni per svolgere le attività di indagine e correzione in maniera totalmente automatizzata.

Log consolidati e centralizzati.

La possibilità di integrare servizi di terze parti per l'aggregazione dei log esterni aiuta i team di sicurezza a identificare le tendenze, analizzare gli eventi dell'infrastruttura, monitorare le anomalie e stabilire le correlazioni fra gli eventi.

Supporto per i servizi delle directory locali e il controllo degli accessi.

Associare i servizi directory degli utenti all'infrastruttura consente ai team di sicurezza di centralizzare l'accesso e l'esecuzione dei processi, assegnare sottogruppi di operazioni a ruoli specifici e condividere le attività con altri gruppi.

Integrazione di app esterne tramite API RESTful.

I team di sicurezza possono avvalersi di Red Hat Ansible Automation Platform per gestire le altre applicazioni aziendali, ad esempio le soluzioni SOAR.

Sfrutta l'automazione per rafforzare la sicurezza della tua azienda.

Scopri di più su Red Hat Ansible Automation Platform.

Informazioni su Red Hat

Red Hat è leader mondiale nella fornitura di soluzioni software open source. Con un approccio che si avvale della collaborazione delle community, distribuisce tecnologie Linux, cloud ibrido, container e Kubernetes caratterizzate da affidabilità e prestazioni elevate. Red Hat consente di sviluppare applicazioni cloud native, integrare applicazioni IT nuove ed esistenti, e automatizzare e gestire ambienti complessi. Considerata un partner affidabile dalle aziende della classifica Fortune 500, Red Hat fornisce pluripremiati servizi di consulenza, formazione e assistenza, che portano i vantaggi dell'innovazione open source in qualsiasi settore. Red Hat è l'elemento catalizzatore in una rete globale di aziende, partner e community, e permette alle organizzazioni di crescere, evolversi e prepararsi a un futuro digitale.

ITALIA

it.redhat.com
italy@redhat.com

EUROPA, MEDIO ORIENTE, E AFRICA (EMEA)

00800 7334 2835
it.redhat.com
europe@redhat.com