Difenditi dalle minacce rilevate dall'IA

> Ogni settimana dobbiamo eseguire scansioni di sicurezza … che elencano le vulnerabilità nei pacchetti presenti sui sistemi operativi. Ogni volta che accade, possiamo consultare immediatamente il sito di Red Hat, dove troviamo una spiegazione completa che ci aiuta a capire se i nostri sistemi ne sono interessati. Nessun altro offre questo livello di supporto per le altre distribuzioni Linux. Senza questo servizio, la gestione di un ambiente di produzione della pubblica amministrazione diventerebbe rapidamente un incubo, perché ogni mese dovremmo svolgere tutte queste attività di ricerca in autonomia.[2]

Ryan Kimbrell,
Senior Cloud Operations Engineer di Zoom[1].

Difendersi dalle vulnerabilità dell'IA

Il panorama delle minacce è cambiato radicalmente. Gli strumenti basati sull'IA individuano oggi potenziali vulnerabilità a un ritmo esponenzialmente superiore rispetto a quello registrato in passato. Già nel 2025 i team di sicurezza aziendali erano sottoposti a una pressione estrema, con una media di 132 CVE individuate ogni giorno.[2] Nel primo trimestre del 2026, questo numero è già aumentato del 26% e la continua evoluzione degli strumenti di IA per l'individuazione delle vulnerabilità, come Mythos, potrebbe mettere in crisi gli approcci tradizionali alla gestione delle CVE.[1]

Nel 2020, i team disponevano in media di un vantaggio di 44 giorni per correggere una vulnerabilità prima che venisse sfruttata.[3] Nel 2025, quel vantaggio si è trasformato in uno svantaggio di 7 giorni.[4] Oggi i criminali informatici possono sfruttare nuove vulnerabilità una settimana prima che venga resa pubblica la relativa CVE.

Nel frattempo, i team di sicurezza enterprise continuano a operare con processi manuali: triage manuale, riunioni di gestione delle modifiche e SLA per il patching che richiedono settimane o addirittura mesi.

Gli approcci tradizionali alla sicurezza IT non riescono più a stare al passo con le attività di triage necessarie per gestire il numero crescente di CVE. In media, nelle grandi organizzazioni il 37% delle vulnerabilità individuate ogni anno non viene corretto e il tempo medio di risoluzione (MTTR) nel settore del software è di 55 giorni.[5] Questa falla nella sicurezza non è sostenibile e mette a dura prova le organizzazioni.

Le quattro principali sfide per i team di sicurezza enterprise di oggi

Al giorno d'oggi le organizzazioni si trovano ad affrontare quattro criticità strettamente interconnesse:

1. **Macchine sempre più veloci.** L'aumento esponenziale delle patch rilasciate dai fornitori può sovraccaricare i team di sicurezza, provocando una grave desensibilizzazione agli avvisi e mettendo sotto pressione i tradizionali flussi di lavoro di gestione delle vulnerabilità.
2. **Sovraccarico di aggiornamenti.** Massive surges in vendor patch releases can overwhelm security teams, triggering severe alert fatigue and straining traditional vulnerability management workflows.
3. **Stabilità o sicurezza.** I team rimandano l'applicazione delle patch per evitare di compromettere il funzionamento delle applicazioni in produzione.
4. **Errori di configurazione.** Gli ambienti tradizionali e gli account con privilegi eccessivi possono dare origine a percorsi sfruttabili dall'IA molto più rapidamente di quanto sia possibile individuarli con le consuete valutazioni manuali.

La soluzione non è introdurre altri software di sicurezza. Per i clienti Red Hat esistenti, è probabile che le funzionalità integrate di correzione delle vulnerabilità siano già presenti nel portafoglio prodotti: devono solo essere attivate.

Crea una base incentrata sulla sicurezza con Red Hat Enterprise Linux

Red Hat® Enterprise Linux® può contribuire a ridurre al minimo gli effetti delle CVE durante le attività di valutazione, test e distribuzione delle patch. La modalità immagine per Red Hat Enterprise Linux distribuisce la piattaforma come un'immagine container firmata e versionata, corredata da una Software bill of materials (SBOM). Inoltre, Security-Enhanced Linux (SELinux) e fapolicyd (File Access Policy Daemon) aggiungono livelli di protezione in fase di runtime che contribuiscono a bloccare l'esecuzione non autorizzata e a confinare i processi compromessi.

Identifica l'esposizione reale con Red Hat Lightspeed

Prima di poter correggere le vulnerabilità in modo scalabile, i team devono sapere a quali rischi sono realmente esposti, non sulla base di un database generico delle vulnerabilità, ma nel proprio ambiente, a seconda delle configurazioni e dei carichi di lavoro effettivamente in uso.

Red Hat Lightspeed aiuta le organizzazioni a stabilire le priorità di intervento sulle CVE nei sistemi Red Hat Enterprise Linux combinando i dati relativi ai pacchetti e agli advisory con regole di sicurezza selezionate da Red Hat, il raggruppamento dei carichi di lavoro e una valutazione che tiene conto della configurazione, considerando anche controlli come SELinux e il livello di esposizione dei servizi. A differenza della scansione basata sulle versioni, distingue i sistemi con vulnerabilità sfruttabili da quelli vulnerabili, ma non effettivamente interessati dalla vulnerabilità. In questo modo i team possono concentrarsi per prima cosa sui rischi su cui è possibile intervenire. Nei test condotti su 90 host, il rilevamento e la correzione automatizzati con Red Hat Lightspeed hanno ridotto fino al 79% il tempo di intervento degli amministratori per la gestione delle CVE e fino all'86% per i problemi operativi noti, rispetto a un approccio basato su script creati manualmente[6].

Questa capacità di valutare le vulnerabilità nel loro contesto è ora più importante che mai. L'enorme volume di vulnerabilità individuate ha dato origine a una nuova forma di paralisi operativa: la desensibilizzazione agli allarmi. Quando centinaia di CVE vengono divulgate nell'arco di poco tempo, nessun team è in grado di valutarle tutte manualmente. Red Hat Lightspeed aiuta a distinguere ciò che conta davvero, consentendo ai team di concentrare gli interventi di correzione sulle vulnerabilità che incidono realmente sul proprio ambiente.

Convalida e gestisci le patch con Red Hat Satellite

Sapere quali vulnerabilità correggere è solo il primo passo. Testare, verificare, approvare e distribuire in produzione la patch corretta, senza introdurre nuove instabilità, richiede un processo controllato e ripetibile.

Red Hat Satellite offre la gestione delle correzioni on premise e lo staging scalabile dei contenuti in infrastrutture locali, ibride e air gap, totalmente insolate. Satellite crea visualizzazioni dei contenuti, ovvero istantanee verificate del software in un determinato momento, e le promuove in modo controllato nei diversi ambienti del ciclo di vita, dallo sviluppo ai test fino alla produzione. Prima di essere distribuite in produzione, le patch devono superare un processo di approvazione definito, così da poter essere verificate in modo approfondito.

Satellite contribuisce inoltre a proteggere la catena di distribuzione del software: i pacchetti introdotti nell'ambiente provengono dai repository verificati di Red Hat e sono firmati crittograficamente. Per le organizzazioni che operano in ambienti altamente regolamentati o isolati, Satellite offre le stesse funzionalità anche in ambienti senza accesso diretto a Internet, consentendo di controllare quale software può essere introdotto nell'infrastruttura. La reportistica sulla conformità viene automatizzata tramite il framework di scansione Open Security Content Automation Protocol (OpenSCAP), che genera report pronti per l'audit in conformità ai requisiti delle integrazioni continue (CI), alle Security Technical Implementation Guides della Defense Information Systems Agency (DISA STIG) e alle baseline degli ambienti sandbox per lo sviluppo conformi agli standard Payment Card Industry (PCI).

Correggi le vulnerabilità in modo scalabile con Red Hat Ansible Automation Platform

Una volta convalidate e preparate le patch per la distribuzione, la sfida finale consiste nell'applicarle in modo coerente in un'infrastruttura ibrida complessa che comprende migliaia di server, molteplici ambienti cloud, data center on premise e ambienti air gap, senza creare un accumulo di attività manuali che rallenti nuovamente le attività di correzione.

Red Hat Ansible® Automation Platform applica le correzioni in modo scalabile nell'intera infrastruttura ibrida, utilizzando il modello Policy as Code (PaC) per garantire coerenza, verificabilità e ripetibilità. Event-Driven Ansible (EDA) automatizza l'intero flusso di lavoro di correzione delle vulnerabilità: quando Satellite completa la sincronizzazione di un repository contenente una nuova patch di sicurezza, un webhook attiva automaticamente Ansible Automation Platform affinché individui i sistemi vulnerabili e avvii il playbook di correzione. I sistemi ad alto rischio possono essere posti automaticamente in quarantena prima ancora che venga distribuita la patch, limitando così l'esposizione durante la fase più critica della risposta all'incidente. Ogni operazione viene eseguita tramite le Red Hat Ansible Certified Content Collection e genera una chiara tracciabilità secondo il modello PaC, contribuendo a soddisfare i requisiti di conformità senza ricorrere a strumenti aggiuntivi.

La soluzione Red Hat per la correzione delle vulnerabilità a circuito chiuso non è una semplice combinazione di prodotti distinti. È un portafoglio integrato di soluzioni, disponibile con un'unica sottoscrizione e supportato da un unico team. Per le organizzazioni che già utilizzano le soluzioni Red Hat, gli strumenti necessari per contrastare le minacce basate sull'IA sono probabilmente già in uso. L'integrazione di queste soluzioni riduce il tempo medio di risoluzione da settimane di attività manuali a poche ore di processi automatizzati, garantendo al tempo stesso una tracciabilità completa e dimostrabile per ogni sistema dell'infrastruttura.

Scopri di più su Red Hat Lightspeed

Vuoi accelerare la correzione delle CVE? Scopri di più su Red Hat Lightspeed.

Scopri di più su Red Hat Satellite

Per saperne di più su come Red Hat Satellite semplifica la gestione delle infrastrutture in modo scalabile, visita la pagina del prodotto.

Ottieni un'automazione completamente ottimizzata

Per scoprire come Red Hat Ansible Automation Platform contribuisce a ridurre gli errori umani nelle attività ripetitive, visita la pagina del prodotto.

1. CVE Program. "Metrics." CVE: Common Vulnerabilities and Exposures, consultato a giugno 2026.
2. Caso cliente Red Hat. "Zoom for Government rafforza la sicurezza con una piattaforma Red Hat". 10 marzo 2023.
3. Blog di Google Cloud. "How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends". 15 ottobre 2024.
4. Blog di Google Cloud. "M-Trends 2026: Data, Insights, and Strategies From the Frontlines". 23 marzo 2026.
5. Edgescan. "2026 Vulnerability Statistics Report" Edgescan, 2026.
6. Principled Technologies, sponsorizzato da Red Hat, "Save administrator time with the automated remediation capabilities of Red Hat Lightspeed", novembre 2025 (versione rivista).

Informazioni su Red Hat

Red Hat è leader mondiale nella fornitura di soluzioni software open source. Con un approccio basato sul concetto di community, distribuisce tecnologie affidabili e ad alte prestazioni per il cloud, lo sviluppo, l'IA, Linux, l'automazione e le piattaforme applicative. Red Hat consente di sviluppare applicazioni cloud native, integrare applicazioni IT nuove ed esistenti, nonché automatizzare e gestire ambienti complessi. Considerata un partner affidabile dalle aziende della classifica Fortune 500, Red Hat fornisce pluripremiati servizi di consulenza, formazione e supporto, 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.

Nord America	1-888-REDHAT1	www.redhat.com	@red-hat
Asia Pacifico	+65 6490 4200	apac@redhat.com	@redhat
America Latina	+54 11 4329 7300	info-latam@redhat.com	@redhat
Europa, Medio Oriente e Africa	00800 7334 2835	europe@redhat.com	@red_hat