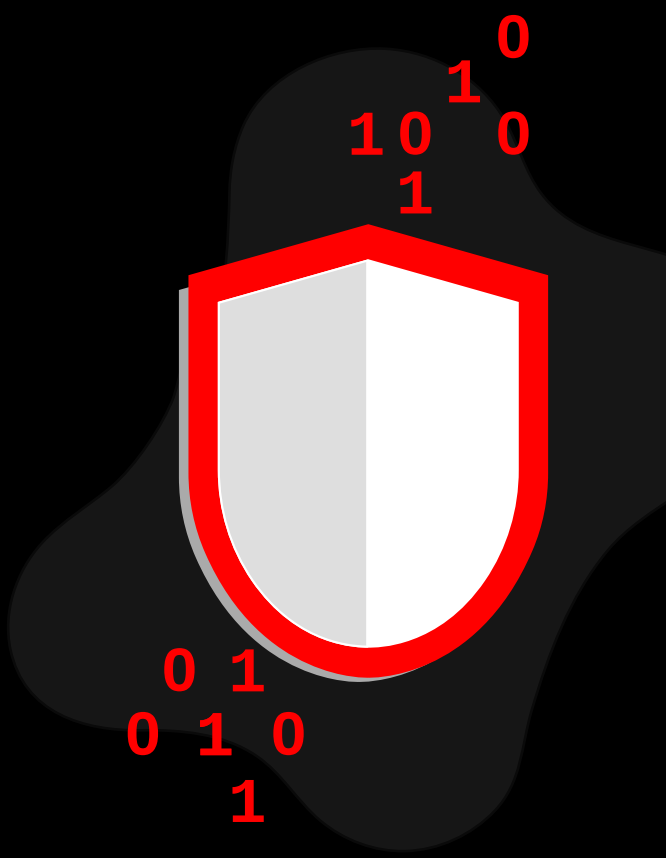
Red Hat

Migliora la sicurezza e la conformità

Riduci i rischi con una piattaforma Linux open source affidabile

Contenuti



Linux: una base solida per il futuro

Linux® è uno dei sistemi operativi più utilizzati al mondo e la piattaforma ideale per ambienti IT moderni e innovativi. Solitamente viene scelto per l'esecuzione di carichi di lavoro critici, che richiedono alti livelli di affidabilità e disponibilità, in datacenter e ambienti cloud e supporta una vasta gamma di scenari di utilizzo, sistemi target e dispositivi. Nei marketplace dei principali provider di cloud pubblico si possono trovare varie distribuzioni Linux.

È bene ricordare che la distribuzione Linux e gli strumenti di gestione che si scelgono possono avere un impatto notevole sull'efficienza, sulla sicurezza e sull'interoperabilità dell'ambiente IT. Questo ebook illustra alcune considerazioni chiave in merito alle vulnerabilità di sicurezza e ai rischi per la conformità più comuni negli ambienti Linux e offre preziosi consigli per gestirli.

L'importanza cruciale di sicurezza e conformità

I rischi per la sicurezza e la conformità dell'ambiente IT sono motivo di preoccupazione in ogni azienda. Il 23% delle organizzazioni ha subito un attacco informatico negli ultimi 2 anni,[1] e come ben sappiamo le violazioni della sicurezza possono costare care. Una violazione dei dati costa in media US$ 4,45 milioni.[2]

Come se non bastasse, le normative statali e settoriali sono in continua evoluzione. Tenere il passo è complicato, ma i problemi di conformità possono aumentare del 5% circa il costo di una violazione dei dati.[2]

Evita le conseguenze di una sicurezza inefficace

Per ridurre il rischio e gli effetti negativi delle violazioni, la velocità è essenziale.

US$ 4,45M
Costo medio di una violazione dei dati nel 2023.[2]

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

US$ 1,02M
Risparmio sui costi ottenibile riuscendo a identificare e contenere una violazione entro 200 giorni.[2]

1 Nash Squared, "2023 Nash Squared Digital Leadership Report", novembre 2023.
2 IBM Security, "Cost of a Data Breach Report 2023", 2023.

Sfide comuni legate alla sicurezza e alla conformità

La gestione della conformità e delle vulnerabilità di sicurezza è ostacolata da molti fattori.

Cambiamento degli scenari di sicurezza e conformità

Le minacce alla sicurezza e le norme di conformità si evolvono rapidamente ed esigono una reazione altrettanto veloce.

23%
delle organizzazioni ha subito un attacco informatico negli ultimi 2 anni.[3]

82%
delle violazioni del 2023 ha coinvolto dati archiviati in ambienti cloud o in più ambienti.[4]

Ambienti cloud distribuiti

In ambienti cloud ibridi e multicloud distribuiti sia geograficamente che logicamente è più complesso avere una visione completa dell'infrastruttura IT e quindi anche applicare configurazioni coerenti in tutti i sistemi.

Ambienti IT ampi e complessi

Nelle infrastrutture di grandi dimensioni vengono spesso utilizzati diversi strumenti per garantire sicurezza e conformità, ma questo complica la gestione dei rischi.

La complessità dei sistemi di sicurezza incrementa il costo di una violazione dei dati di

US$ 240.889.[4]

La forza lavoro remota incrementa il costo medio di una violazione dei dati di

US$ 173.074

rispetto alle violazioni che non coinvolgono il lavoro da remoto.[4]

Personale limitato e direttive sul lavoro da remoto

La maggior parte delle aziende non dispone del personale necessario per gestire manualmente le attività relative a conformità e sicurezza, e il lavoro da remoto complica la tutela dei dispositivi e dei punti di accesso alle risorse digitali dell'organizzazione.

*3 Nash Squared, "**2023 Nash Squared Digital Leadership Report**", novembre 2023.*
*4 IBM Security, "**Cost of a Data Breach Report 2023**", 2023.*

Un approccio efficace per la gestione di sicurezza e conformità

Per gestire le vulnerabilità di sicurezza e la conformità è necessario monitorare e valutare i sistemi allo scopo di verificare che rispettino le normative e i criteri di sicurezza. L'approccio ideale per la gestione delle vulnerabilità di sicurezza e della conformità dovrebbe consentire lo sviluppo di processi coerenti e ripetibili nell'intero ambiente per svolgere le seguenti attività:

Valutazione

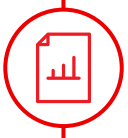
Individua i sistemi non conformi o vulnerabili. Valuta il livello di sicurezza dell'ambiente, dall'infrastruttura ai singoli carichi di lavoro, per identificare gli avvisi di sicurezza effettivamente applicabili al tuo ambiente e ai tuoi sistemi.

Definizione delle priorità

Organizza le attività di correzione in base all'impegno richiesto, all'impatto e alla gravità del problema. Utilizza le tecniche di gestione dei rischi per identificare i rischi aziendali effettivamente associati a ciascun problema e pianifica le misure correttive di conseguenza. Per valutare il rischio è necessario determinare la probabilità che un problema dia origine a una violazione, la gravità potenziale di tale violazione e le implicazioni della risoluzione del problema. Potrebbe non avere senso risolvere un determinato problema nei sistemi di sviluppo e test, ma quello stesso problema potrebbe costituire una priorità nei sistemi di produzione.

Correzione

Applica le patch e riconfigura tempestivamente i sistemi sui quali è necessario intervenire. Automatizza i processi di configurazione e gestione delle patch per accelerare la correzione, garantire coerenza fra i sistemi e ridurre il rischio di errore umano. Se utilizzati efficacemente, gli strumenti automatizzati consentono di risolvere i problemi velocemente e di migliorare la sicurezza dell'ambiente e dell'intera azienda.



Report

Verifica che le modifiche siano state applicate e automatizza la generazione dei report per semplificare gli audit. Un'attività di reporting efficace permette di fornire informazioni complete al fine di consentire a dirigenti di alto livello, auditor e team tecnici di comprendere le esposizioni e i rischi attuali per la sicurezza.

Questo approccio prepara inoltre l'azienda ad adottare tecniche di sviluppo e gestione moderne e in rapida evoluzione, come DevSecOps. Nelle sezioni successive vengono illustrate le considerazioni e le misure più importanti per gestire efficacemente i rischi per la sicurezza e la conformità.

Identificazione ed eliminazione delle vulnerabilità negli ambienti Linux

Per identificare ed eliminare le vulnerabilità è necessario valutare l'infrastruttura allo scopo di trovare e correggere i sistemi che risultano vulnerabili agli attacchi. Tali vulnerabilità possono essere dovute a nuove minacce, patch obsolete o mancanti, o ad errori di configurazione dei sistemi. Gli interventi correttivi includono solitamente l'applicazione delle patch, l'aggiornamento e la riconfigurazione dei sistemi, al fine di eliminare le vulnerabilità.

Perché è importante?

Le vulnerabilità di sicurezza possono causare costose violazioni, con il rischio di compromettere la fiducia dei clienti, la reputazione dell'azienda e il fatturato. Infatti, la perdita di opportunità commerciali rappresenta il 29,2% del costo medio di una violazione dei dati.[5]

Ostacoli che impediscono di identificare ed eliminare efficacemente le vulnerabilità

Nella maggior parte delle aziende manca una strategia di sicurezza coerente per le operazioni su vasta scala.

- Lo scarso personale disponibile è sovraccarico di lavoro e potrebbe non disporre delle competenze necessarie per sviluppare ed eseguire una strategia di sicurezza completa.
- Gli strumenti di scansione della sicurezza generici producono interminabili elenchi di vulnerabilità potenziali, ma non tutte sono applicabili al tuo ambiente e il personale è costretto a dedicare moltissimo tempo alla ricerca delle vulnerabilità e alle azioni correttive.
- L'utilizzo di strumenti manuali per l'identificazione, la correzione e i processi di tracciamento rallentano le operazioni, e le vulnerabilità note rimangono spesso prive di patch.
- I metodi di correzione ad hoc determinano un'applicazione incoerente delle patch e incrementano i potenziali rischi per la sicurezza.

5 IBM Security, "Cost of a Data Breach Report 2023", 2023.

Funzionalità principali degli strumenti di gestione della sicurezza

Per garantire una sicurezza efficace occorre identificare e correggere rapidamente le vulnerabilità dei sistemi prima che si verifichi una violazione. Cerca strumenti unificati di gestione della sicurezza che offrono:

Analisi dei sistemi per identificare i rischi, sia a livello di sistema operativo che di carico di lavoro, nei sistemi e nelle istanze di tutto l'ambiente.

Correzione automatizzata dei rischi identificati per migliorare la velocità, la precisione e l'efficienza dei team IT e di sicurezza.

Comprovata esperienza del fornitore che saprà dare utili consigli sull'utilizzo dei prodotti, ad esempio suggerire l'applicazione di semplici misure correttive per ridurre i rischi.

Accesso regolare ai dati più recenti sulle vulnerabilità note e sui rischi per la sicurezza forniti dal sistema operativo e dai fornitori delle applicazioni.

Generazione di report relativi a rischi potenziali, azioni correttive e audit, con il livello di dettaglio più appropriato ai diversi tipi di destinatari.

Gestione della conformità negli ambienti Linux

La gestione delle conformità ha lo scopo di verificare la conformità dei sistemi alle policy aziendali, agli standard settoriali e alle normative applicabili in un determinato momento. Valuta l'infrastruttura per individuare i sistemi che risultano non conformi a causa delle modifiche apportate a normative, policy o standard, a causa di configurazioni errate o per altri motivi.

Perché è importante?

Oltre alle violazioni della sicurezza, i problemi di conformità possono determinare sanzioni, danni all'azienda e la perdita di certificazioni. I problemi di conformità aumentano il costo medio delle violazioni dei dati.[6]

Ostacoli a una gestione efficace della conformità

Per gestire la conformità molte aziende utilizzano operazioni manuali e script personalizzati, ma questi processi sono troppo lenti e hanno un impatto limitato per i moderni ambienti operativi e di sviluppo in rapida evoluzione.

- A causa dei numerosissimi dati di riferimento e standard generici, è difficile comprenderne la rilevanza e l'impatto sull'ambiente.
- I processi manuali rallentano il monitoraggio della conformità, la correzione e le operazioni di auditing, il che porta a un impiego inefficiente del personale, un'applicazione incoerente delle policy e un rischio maggiore di introdurre problemi di conformità.
- Molte aziende usano diversi strumenti per gestire la sicurezza e la conformità, ma questo riduce l'efficienza operativa e ostacola la configurazione di policy personalizzate coerenti.

Funzionalità principali degli strumenti di gestione della conformità

Per garantire una conformità efficace occorre definire e applicare policy contestuali, assicurare che i sistemi rispettino tali policy e generare e gestire velocemente i report sulla conformità per gli audit. Cerca strumenti unificati di gestione della conformità che offrono:

Funzionalità di analisi con cui identificare i rischi per la conformità in modo coerente, senza sprecare tempo.

Correzione automatizzata dei sistemi non conformi.

Un quadro completo del livello di conformità nell'intero ambiente.

Generazione automatica di report sulla conformità, in base ai tuoi requisiti di auditing e alle esigenze dei destinatari.

Consigli specialistici e indicazioni contestuali per correggere i sistemi non conformi nell'intero ambiente.

6 *IBM Security, "Cost of a Data Breach Report 2023", 2023.*

Best practice e strumenti consigliati

Analizza regolarmente i sistemi

Il monitoraggio quotidiano può aiutarti a identificare le vulnerabilità e i rischi per la conformità prima che interrompano le operazioni aziendali e determinino una violazione. Assicurati di utilizzare i dati più recenti sulla sicurezza forniti dal sistema operativo e dai fornitori delle applicazioni per migliorare la precisione delle analisi e configura criteri di sicurezza adatte al tuo ambiente e ai tuoi processi, per generare risultati di conformità più accurati.

Identificare e contenere una violazione entro

200 giorni

riduce in maniera significativa il costo della violazione.[7]

Applica e testa le patch di frequente

L'aggiornamento regolare dei sistemi consente di migliorarne i livelli di sicurezza, l'affidabilità, le prestazioni e la conformità. Applica le patch regolarmente e tieniti informato sui problemi importanti in generale. Applica tempestivamente le patch per i bug e i difetti critici. Esegui un test dei sistemi a cui sono state applicate le patch prima del passaggio in produzione.

Uno strumento di gestione efficace accelera l'applicazione delle patch ai sistemi del

56%.[8]

Adotta soluzioni di automazione

A mano a mano che le dimensioni e la complessità dell'infrastruttura aumentano, diventa più difficile gestirla manualmente. L'automazione consente di semplificare il monitoraggio, accelerare la correzione, migliorare la coerenza e garantire un'attività di reporting regolare.

L'automazione della sicurezza e l'intelligenza artificiale (IA) possono ridurre il costo di una violazione dei dati del

39,3%.[7]

7 IBM Security, "Cost of a Data Breach Report 2023", 2023.

8 White paper di IDC, sponsorizzato da Red Hat, "Red Hat Satellite Helps Enterprise Organizations Optimize Infrastructure with Automation Tools", documento n. US46109220, agosto 2021.

Connetti gli strumenti e allinea i processi

Spesso, negli ambienti distribuiti vengono utilizzati strumenti di gestione diversi a seconda della piattaforma. Integra tali strumenti utilizzando le interfacce di programmazione delle applicazioni (API) e usa le tue interfacce preferite per eseguire attività in altri strumenti. Riduci il numero delle interfacce in uso, per semplificare le operazioni e aumentare la visibilità sulle condizioni di sicurezza e conformità di tutti i sistemi dell'ambiente. Infine, allinea i processi fra i diversi ambienti per aumentare i livelli di coerenza e affidabilità.

La complessità dei sistemi di sicurezza incrementa il costo medio di una violazione dei dati del

31,6%.[9]

Adotta una strategia di sicurezza continua e coerente

Per ottenere una sicurezza efficace occorre adottare un approccio olistico, che tiene conto di persone, processi e tecnologie. Una strategia di sicurezza continua richiede feedback e adattamento per supportare le moderne tecniche di sviluppo DevSecOps e le esigenze delle aziende digitali. Adotta un approccio alla sicurezza stratificato e misure di difesa avanzate per sfruttare al meglio le funzionalità di ogni livello dell'ambiente, inclusi sistemi operativi, piattaforme container, strumenti di automazione, soluzioni Software as a Service (SaaS) e servizi cloud.

L'adozione di un approccio DevSecOps può ridurre il costo medio di una violazione dei dati del

38,4%.[9]

9 *IBM Security,* "Cost of a Data Breach Report 2023", *2023.*

Gli strumenti ideali per la sicurezza e la conformità devono offrire numerose funzioni e capacità chiave.

Analisi proattiva

Per migliorare il livello di sicurezza e conformità, occorre innanzitutto conoscerlo. Gli strumenti che eseguono analisi automatizzate garantiscono il monitoraggio regolare dei sistemi e l'invio di notifiche in caso di problemi, il che agevola e sveltisce il lavoro del personale.

Definizione delle priorità

Gli strumenti che forniscono istruzioni prescrittive per le correzioni eliminano la necessità di ricercare le misure da adottare a posteriori, il che permette di risparmiare tempo e ridurre il rischio di errore. Attribuendo le priorità agli interventi in base all'impatto potenziale e ai sistemi interessati, è possibile ottimizzare i tempi di correzione.

Risultati personalizzabili

Su alcuni sistemi non è possibile eseguire determinati controlli di vulnerabilità e conformità a causa di configurazioni, utilizzi e carichi di lavoro specifici. È consigliabile utilizzare strumenti che consentono di definire il contesto aziendale per ridurre i falsi positivi, gestire i rischi e ottenere una visione realistica delle condizioni di sicurezza e conformità.

Report intuitivi

Gli strumenti che generano report chiari e intuitivi dai quali siano evidenti i sistemi su cui sono state applicate le patch, quelli su cui occorre ancora intervenire e quelli non conformi ai criteri di sicurezza aumentano le capacità di controllo e consentono di comprendere meglio le condizioni dell'ambiente.

Interfaccia unificata

Utilizzando strumenti che non si limitano alla gestione di un singolo componente o livello dell'ambiente è possibile semplificare le operazioni di sicurezza e migliorare la comprensione dei livelli di sicurezza e conformità. Gli strumenti unificati possono inoltre fornire ulteriore contesto per le scansioni e indicazioni per la correzione.

Un piano d'azione attuabile

Gli strumenti che forniscono informazioni su misura per l'ambiente possono aiutarti a identificare più rapidamente i potenziali problemi di conformità e vulnerabilità di sicurezza, i sistemi interessati e una previsione dell'impatto. Tali strumenti consentono anche di pianificare le azioni correttive e definirne le priorità.

Aumenta i livelli di sicurezza e conformità con Red Hat

Red Hat adotta un approccio olistico alla gestione dei rischi per la sicurezza e la conformità che migliora i livelli di velocità, scalabilità e stabilità nell'intero ambiente IT, dai server bare metal e virtualizzati, all'infrastruttura di cloud privato, pubblico e ibrido, fino ai deployment all'edge. Integrando persone, processi e tecnologia, le piattaforme Red Hat® aiutano a migliorare l'efficienza operativa, promuovere l'innovazione e aumentare la soddisfazione dei dipendenti.

L'elemento centrale della strategia è costituito da **Red Hat Enterprise Linux**, una piattaforma operativa coerente e intelligente che fornisce una base per i moderni deployment IT e di cloud ibrido, massimizzando i vantaggi per l'azienda. Un'infrastruttura coerente permette di distribuire applicazioni, carichi di lavoro e servizi ovunque utilizzando gli stessi strumenti.

La sicurezza costituisce un elemento fondamentale dell'architettura e del ciclo di vita di Red Hat Enterprise Linux. L'approccio stratificato di difesa contro le violazioni prevede controlli di sicurezza automatizzati e ripetibili per limitare il rischio di esposizione alle vulnerabilità. Gli aggiornamenti critici per la sicurezza e le patch live, forniti nell'ambito della sottoscrizione Red Hat Enterprise Linux, garantiscono un ambiente sempre aggiornato e più sicuro.

> Red Hat Enterprise Linux ci consente di **rilevare e analizzare i bug e le vulnerabilità in modo più efficiente** rispetto alla distribuzione Linux che utilizzavamo in precedenza.[10]
>
> **Yuki Miyamoto**
> IT Infrastructure/Business Online Infrastructure System, Information Technology Division, Square Enix Co., Ltd.

*10 Caso cliente di Red Hat, "**Square Enix semplifica la gestione dell'infrastruttura per il gaming online**", maggio 2023.*

Gli strumenti di gestione Red Hat si integrano con Red Hat Enterprise Linux allo scopo di offrire le funzionalità necessarie per gestire efficacemente i rischi associati alle vulnerabilità di sicurezza e alla conformità.

Le baseline e gli strumenti configurabili riducono i falsi positivi e forniscono una visione accurata delle condizioni dell'infrastruttura.

Le funzionalità di automazione migliorano la configurazione, consentono di gestire le patch in modo più preciso e riducono il rischio di errore umano.

Le viste personalizzabili consentono di ottenere rapidamente le informazioni giuste per ciascun utente al momento giusto.

La correzione automatizzata e proattiva consente di risolvere i problemi più velocemente, senza richiedere l'intervento del supporto tecnico.

Una libreria di risorse esaustiva offre l'accesso continuo a informazioni dettagliate e specifiche.

Le opzioni di deployment in loco e Software as a Service (SaaS) consentono di installare gli strumenti nel modo desiderato.

Le API si collegano alle interfacce e agli strumenti di sicurezza, conformità e gestione che preferisci.

Le funzionalità per il rilevamento di vulnerabilità e malware analizzano i sistemi alla ricerca di Common Vulnerabilities and Exposures (CVE) e firme malware.

Le funzionalità di ottimizzazione delle risorse consentono di ottimizzare i deployment nel cloud pubblico grazie alle metriche sulle prestazioni di reti, memorie e processori.

Sfrutta gli strumenti integrati

Gli strumenti di gestione Red Hat sono basati su anni di esperienza in materia di sviluppo e supporto di Linux. Operano in sinergia per semplificare l'amministrazione dell'IT, aiutano i team a risparmiare tempo ed energie e migliorano i livelli di sicurezza, ottimizzazione e affidabilità dell'ambiente.

Red Hat Insights

Analizza, osserva e gestisci i sistemi Red Hat

Red Hat Insights, una soluzione inclusa in Red Hat Enterprise Linux e fornita come servizio, esegue un'analisi continua delle piattaforme e delle applicazioni. Prevede i rischi, suggerisce le azioni da intraprendere e monitora i costi in modo da assicurare una gestione ottimale degli ambienti cloud ibridi. Insights permette di monitorare l'efficienza, la stabilità e le prestazioni dell'IT, gestire i rischi per la sicurezza e la conformità e ottimizzare le spese negli ambienti cloud.

Scopri di più su Insights

+26% di velocità nella risoluzione degli incidenti di sicurezza[11]

+24% di efficienza dei team dedicati alla sicurezza dell'IT[11]

-76% di tempi di fermo non pianificati[11]

Red Hat Satellite

Semplifica e automatizza la gestione dei sistemi

Red Hat Satellite è una soluzione di gestione dell'infrastruttura ideale per il provisioning e la manutenzione dei sistemi Red Hat Enterprise Linux in qualsiasi ambiente: fisico, virtuale, cloud o edge. Satellite semplifica il provisioning, l'applicazione delle patch e altre attività ripetitive legate alla gestione e alla scalabilità dei sistemi. Aiuta a incrementare l'efficienza operativa e a garantire la sicurezza, la disponibilità e la conformità dei sistemi.

Scopri di più su Satellite

+56% di efficienza nell'applicazione delle patch[12]

+56% di efficienza nell'infrastruttura IT[12]

-28% nel costo delle operazioni[12]

11 Sintesi di IDC sul valore aziendale, sponsorizzata da Red Hat, "The Business Value of Red Hat Insights", documento n. US51795124, febbraio 2024.

12 White paper di IDC, sponsorizzato da Red Hat, "Red Hat Satellite Helps Enterprise Organizations Optimize Infrastructure with Automation Tools", documento n. US46109220, agosto 2021.

Storia di successo

Met Office

Il Meteorological Office, ovvero il servizio meteorologico nazionale del Regno Unito, fornisce quotidianamente servizi relativi al meteo e alle condizioni climatiche in tutto il mondo. Alla ricerca di un approccio globale per la gestione dei server, Met Office ha adottato Red Hat Insights da utilizzare in combinazione con Red Hat Satellite. Inoltre, grazie al supporto di un Red Hat Technical Account Manager, l'azienda è riuscita a migliorare in maniera significativa la visibilità sull'ambiente server.

Met Office ha innanzitutto utilizzato Insights per esaminare numerose macchine che presentavano problemi noti. Le criticità sono state rilevate immediatamente e il team IT ha quindi deciso di procedere a un deployment più ampio. In questo caso il team ha utilizzato Satellite, in conformità con i processi interni di gestione delle modifiche, per semplificare l'installazione di Insights in tutti i sistemi.

Insights ha contribuito a semplificare l'assegnazione delle priorità, il rilevamento dei problemi, l'individuazione dei sistemi compromessi e il riconoscimento della gravità dei problemi. Inoltre, ha aiutato Met Office a portare i propri server a uno standard desiderato identificando e risolvendo i problemi di configurazione.

Met Office continuerà a utilizzare Insights e Satellite per gestire l'intero ambiente e migliorarne la sicurezza in maniera proattiva.

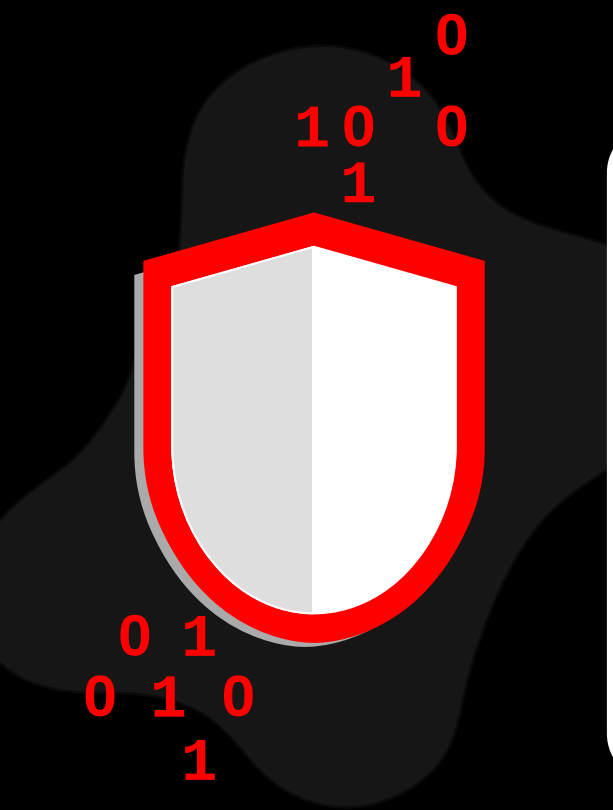
> Ho capito che Red Hat Insights poteva offrirci maggiore visibilità e ci dava l'opportunità di adottare un **approccio olistico alla gestione dell'intero ambiente**. Red Hat Satellite è la soluzione perfetta per rilevare i problemi sulle singole macchine, mentre il punto di forza di Red Hat Insights sta nella sua capacità di identificare problemi comuni tra i sistemi.
>
> **Chris Wilkinson**
> Senior Systems Engineer,
> The Meteorological Office, U.K.

Leggi la storia di successo

Inizia il tuo percorso

Le applicazioni e l'infrastruttura IT sono fondamentali per il successo dell'azienda. Adottando approcci e strumenti efficaci per la gestione delle vulnerabilità di sicurezza e dei rischi per la conformità, è possibile proteggere la propria organizzazione.

Red Hat fornisce la piattaforma Linux affidabile e gli strumenti di gestione integrati necessari per operazioni e innovazione incentrate sulla sicurezza.



Analizza i rischi con Red Hat Insights

- **Scopri di più** su Red Hat Insights
- **Leggi il resoconto analitico** su Red Hat Insights

Gestisci i sistemi su larga scala con Red Hat Satellite

- **Scopri di più** su Red Hat Satellite
- **Leggi il resoconto analitico** su Red Hat Satellite

1156696_0524_KVM

Red Hat