Migliorare la compliance informatica con l'automazione dell'infrastruttura

Monitora gli eventi su più agenzie. Automatizza la risposta con il playbook di ogni agenzia.

Le soluzioni di Red Hat

Red Hat Integration connette i dati raccolti dai server e dai dispositivi edge e di rete di diverse agenzie.

Open Data Hub su Red Hat OpenShift ti consente di addestrare i modelli di apprendimento automatico a riconoscere pattern sospetti.

Red Hat Decision Manager associa gli eventi di sicurezza alle risposte adeguate in base alle regole di ciascuna agenzia.

Red Hat Ansible Automation Platform richiede automaticamente l'intervento dell'agenzia, in base al suo playbook, quando una minaccia viene rilevata.

Il malware non rispetta le distinzioni di ruolo

Le agenzie delle forze dell'ordine del governo federale americano devono proteggere le informazioni sensibili, come indagini, precedenti penali, dati biometrici, dichiarazioni fiscali, registrazioni di videocamere di sorveglianza e documenti sul personale. La rivelazione di dati sensibili può causare interruzioni operative, mettere in pericolo il personale e minare la fiducia nelle istituzioni. Tra gli attacchi più comuni sono inclusi l'esfiltrazione di dati e il Denial-of-Service.

Il rispetto della conformità informatica da parte delle forze ordine incontra una serie di ostacoli, tra cui:

- **Personale limitato.** Le forze dell'ordine non dispongono delle risorse necessarie per monitorare il volume crescente del traffico di dati, inclusi gli stream di dispositivi edge (come le fotocamere IP) che possono essere infettati da malware. La vulnerabilità di questi dispositivi aumenta in caso di ritardi nella rilevazione e nella risoluzione delle minacce.
- **Assenza di monitoraggio centrale delle agenzie.** Spesso gli attacchi contro più agenzie che svolgono sono più sofisticati e hanno più probabilità di causare fughe di dati e interruzioni delle attività aziendali. È facile che un'agenzia sottovaluti la gravità di un evento di sicurezza se ignora che tale evento è parte di un attacco contro più agenzie.
- **La risoluzione non può interrompere le operazioni.** Spesso le forze dell'ordine non riescono a eseguire l'arresto di un dispositivo compromesso senza causare un'interruzione delle operazioni. È quindi necessario un metodo di risoluzione più complesso, che sia equilibrato rispetto alla gravità della minaccia.

Soluzione: una visione globale degli eventi di rete e una risposta automatizzata

La protezione dei dati pubblici richiede due elementi di cui oggi le forze dell'ordine non dispongono. Il primo è la capacità di avere una visione globale dell'attività di server e rete in più organizzazioni. Il secondo è la risoluzione automatizzata basata sul tipo di minaccia e sul playbook dell'agenzia. Gli esempi includono l'applicazione della stessa lista di indirizzi di rete bannati in più agenzie, l'invio di avvisi in caso tali indirizzi vengano rilevati, la messa in quarantena di un carico di lavoro sospetto fino a quando potrà essere analizzato e la terminazione di un server virtuale che mostra comportamenti anomali, seguita dalla messa in funzione di un nuovo server che proviene da una fonte affidabile.

I vantaggi della conformità informatica automatizzata per le forze dell'ordine includono:

- Rilevazione più rapida degli imprevisti.
- Correzione più rapida, che riduce la finestra di vulnerabilità.
- Requisiti delle risorse ridotti per la gestione delle minacce.
- Maggiore soddisfazione sul lavoro, perché i professionisti che si occupano di sicurezza informatica possono tralasciare attività monotone di monitoraggio per dedicarsi a compiti di maggiore valore, il che favorisce le assunzioni e la fidelizzazione dei dipendenti.

facebook.com/RedHatItaly
twitter.com/RedHatItaly
linkedin.com/company/red-hat

Perché scegliere Red Hat?

Maggiore sicurezza. Le nostre soluzioni soddisfano rigorosi requisiti di sicurezza.

Ecosistema dei partner. Collabora con i nostri partner per collegare le soluzioni per l'interrogazione dei dati e la correzione automatizzata.

Collaudata dal governo federale degli Stati Uniti. DHS, DoD e altre agenzie civili americane utilizzano Red Hat OpenShift.

Flessibilità con le API open source. Quando aggiungi un nuovo dispositivo, utilizza anche le API open source per monitorarlo.

Costi ridotti. Le nostre sottoscrizioni possono costare meno delle licenze di software proprietari e dei contratti di supporto.

L'approccio di Red Hat alla conformità informatica automatizzata

Offriamo una soluzione completa per rafforzare la conformità informatica tramite l'automazione dell'infrastruttura.

Addestra un modello di apprendimento automatico a distinguere tra attività normali e anomale. Utilizza la piattaforma di IA Open Data Hub su Red Hat® OpenShift®. Testa il modulo sottoponendogli delle minacce simulate. Affina costantemente il modello trasmettendo dati sulle minacce scoperte di recente e sull'efficacia delle risposte.

Individua le attività di correzione appropriate per ogni tipo di minaccia. Usa Red Hat Decision Manager per specificare le risposte, come il blocco dell'indirizzo IP di un attore malevolo, la definizione del traffico autorizzato, la messa in quarantena di un carico di lavoro, la disattivazione di un server virtuale infetto e l'attivazione di un nuovo server.

Automatizza il monitoraggio e la risposta (in più agenzie). Usa Red Hat Ansible® Automation Platform per raccogliere da più corpi di polizia i log di firewall, ID, dispositivi edge e prodotti di ecosistema come Sensu per l'aggregazione dei log. Puoi anche usare ServiceNow per la gestione delle attività. Ansible Automation Platform avvia in automatico la richiesta di un'azione specifica dal playbook. Se l'azione non risolve il problema, Ansible Automation Platform invia un avviso e apre un caso su ServiceNow.

Consenti alle forze dell'ordine di controllare i propri playbook. Ogni corpo di polizia sa quale livello di rischio è in grado di tollerare prima di dover interrompere un determinato servizio. Con Ansible Automation Platform, i team di sicurezza informatica possono utilizzare un'interfaccia web per modificare le soglie, i nomi host e i playbook per soddisfare i requisiti della missione.

Scopri di più. Per scoprire di più su come Red Hat può supportare l'innovazione delle strutture IT governative, visita redhat.com/government.

Informazioni su Red Hat

Red Hat è leader mondiale nella fornitura di soluzioni software enterprise open source. Con un approccio basato sul concetto di community, distribuisce tecnologie come Kubernetes, container, Linux e cloud ibrido caratterizzate da affidabilità e prestazioni elevate.Red Hat favorisce l'integrazione di applicazioni nuove ed esistenti, lo sviluppo di applicazioni cloud native, la standardizzazione su uno dei principali sistemi operativi enterprise, e consente di automatizzare e gestire ambienti complessi in modo sicuro. I pluripremiati servizi di consulenza, formazione e assistenza hanno reso Red Hat un partner affidabile per le aziende della classifica Fortune 500. Lavorando al fianco di fornitori di servizi cloud e applicazioni, integratori di sistemi, clienti e community open source, Red Hat prepara le organizzazioni ad affrontare 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

facebook.com/RedHatItaly
twitter.com/RedHatItaly
linkedin.com/company/red-hat

it.redhat.com
#F26748_0121