Espandere su scala le forze operative speciali con l'automazione

L'esigenza di un'automazione scalabile

I processi manuali di configurazione del server e di applicazione delle patch richiedono molto tempo e sono soggetti a errori. Per mitigare questi problemi, le organizzazioni del settore pubblico di tutto il mondo, comprese le forze operative speciali (SOF), devono passare a soluzioni di automazione scalabili. L'automazione della configurazione e dell'applicazione di patch evita gli errori manuali, rafforza la sicurezza, accelera la distribuzione di nuove funzionalità e consente al personale di dedicarsi ad attività strategiche di maggior valore. Una soluzione completa che include Red Hat® Ansible® Automation Platform è in grado di automatizzare la configurazione e l'applicazione di patch a tutti i prodotti hardware e software, consolidando gli strumenti specifici per fornitore in un'unica interfaccia unificata.

Il costo dei processi di difesa manuale

Anche quando gli upgrade della rete sono automatizzati, la configurazione e l'applicazione di patch a server, macchine virtuali (VM) e risorse cloud vengono comunque eseguite manualmente. Questo ostacola in modo diretto gli obiettivi strategici della difesa, perché genera:

- Operazioni estremamente laboriose. Le attività manuali ripetitive, come il provisioning di 100 nuovi server o l'applicazione urgente di patch di sicurezza a 200 VM, distolgono il personale da iniziative strategiche critiche, come la Multi-Domain Operations (MDO) Alliance, un'iniziativa della NATO con l'obiettivo di realizzare un framework di sicurezza informatica zero trust entro il 2030.[1]
- Rischio di errori mission-critical. I complessi manuali di istruzioni per gli upgrade e le patch introducono un elevato rischio di errore umano, che può creare vulnerabilità di sicurezza significative o causare un guasto completo del sistema.
- Allocazione errata delle competenze. Spostare gli amministratori dalle attività ripetitive a quelle più creative consente di sfruttare al meglio le loro competenze e di sollevare il morale.

Svantaggi di un'automazione incoerente

Forse la tua agenzia ha automatizzato alcuni processi manuali, ma vorrebbe accelerare il progresso. Una delle principali difficoltà per molti team è che la maggior parte degli strumenti di automazione è specifica per il prodotto di un singolo fornitore. Non è pratico per i team IT dover imparare a usare e gestire più strumenti, uno per ogni VM, server fisico e singola applicazione.

Un altro ostacolo è che i team IT devono avere la certezza di poter mantenere il controllo dei propri processi. Con così tante risorse condivise, ogni team deve giustamente impedire a persone e sistemi di modificare i processi che proteggono le proprie risorse e le loro prestazioni ottimali.

1 *"NATO's Bold Digital Leap: A SECURE Cloud-Empowered Alliance", NATO Allied Command Transformation, 9 dicembre 2024.*

Soluzioni open source per l'automazione e l'orchestrazione

Automatizzando la configurazione e l'applicazione delle patch di hardware e software, i team IT delle SOF possono apportare modifiche una volta e poi trasferirle su tutti o alcuni dispositivi con il minimo sforzo. Se la modifica non funziona come previsto, ripristinare la configurazione a uno stato operativo noto è altrettanto semplice.

Ansible Automation Platform consente alle SOF di automatizzare la configurazione e l'applicazione di patch a tutti i sistemi hardware e software e di orchestrare i flussi di lavoro avanzati. Può automatizzare qualsiasi azione possa essere avviata da un'interfaccia a riga di comando (CLI) o da un'interfaccia di programmazione delle applicazioni (API) per qualsiasi prodotto hardware o software. I moduli Ansible possono essere ottenuti in tre modi diversi:

1. Scarica i moduli dal Red Hat Ecosystem Catalog. Red Hat verifica e cura moduli Ansible in collaborazione con oltre 60 fornitori indipendenti. Tali moduli sono disponibili nel Red Hat Ecosystem Catalog come Ansible Content Collections.
2. Acquista i moduli dai fornitori di software e hardware. Alcuni fornitori pubblicano o mettono a disposizione moduli Ansible per gestire i propri prodotti.
3. Fai da te. Se Red Hat o un altro fornitore non fornisce un modulo per un determinato prodotto, puoi scriverne uno personalizzato.

Con Ansible Automation Platform i team IT possono affrontare le sfide relative al controllo degli accessi per configurazioni e processi. Gli amministratori che avviano un processo da Ansible Automation Platform, come il patching di un server o l'upgrade di un software, non accedono effettivamente alla risorsa. Ansible Automation Platform richiama invece le azioni definite dal team proprietario della risorsa interessata. Solo il team proprietario di una risorsa può accedervi, evitando rischi per la sicurezza come errori di configurazione o escalation dei privilegi.

Scenari di utilizzo di Red Hat Ansible Automation Platform per le SOF

Accesso alla rete a tempo limitato

Immagina che un collaboratore esterno abbia bisogno di accedere a un sistema per 24 ore o che un modello di machine learning debba acquisire dati da una sorgente esterna per 48 ore. Entrambi gli scenari richiedono l'apertura delle porte del firewall. Oggi, gli amministratori devono impostare un promemoria per chiudere le porte allo scadere del tempo. Se l'amministratore non vede il promemoria o è impegnato con un'altra attività, la porta rimane aperta: una vulnerabilità di sicurezza. Con Ansible Automation Platform, gli amministratori possono specificare quando terminare il processo al momento dell'avvio.

Provisioning di risorse a tempo limitato

A volte i team hanno bisogno di aumentare una funzionalità per un breve periodo di tempo, ad esempio il provisioning di risorse cloud classificate per supportare una missione delle forze operative speciali (SOF). Se l'amministratore trascura di ridimensionare le risorse una volta completata la missione, questa negligenza potrebbe comportare costi inutili per settimane o mesi. Con Ansible Automation Platform, l'amministratore può inserire il tempo necessario per il provisioning e il rilascio delle risorse.

Risposta agli incidenti

Attualmente i team di sicurezza mitigano le minacce un dispositivo alla volta, ad esempio applicando una patch, chiudendo una porta o rimuovendo utenti. Queste attività manuali sono particolarmente laboriose, e i dispositivi restano vulnerabili in attesa del proprio turno. Con Ansible Automation Platform, puoi intervenire in modo simultaneo su tutti i dispositivi vulnerabili.

Attività basate sugli eventi

Integrato con altri sistemi delle SOF, Ansible Automation Platform è in grado di rilevare gli eventi in un sistema e di richiamare automaticamente le azioni definite in un altro. Di seguito alcuni esempi:

- **Soddisfare una richiesta per una VM.** In genere, la creazione di una VM richiede meno di 10 minuti. Tuttavia, in molte organizzazioni, tra la richiesta e la produzione possono passare settimane, se non mesi. Un team esegue il provisioning della VM, un altro assegna un indirizzo IP, un altro ancora il sistema operativo e un altro ancora le applicazioni. Ogni fase del flusso di lavoro comporta ritardi. Con Ansible Automation Platform, la richiesta di una VM attiva i processi già definiti da ciascun team, che vengono eseguiti nell'ordine designato. La richiesta della VM può essere soddisfatta in un giorno, se non in un'ora.
- **Automazione del provisioning dei server con Infrastructure as Code (IaC).** Gli sviluppatori delle SOF possono eseguire manualmente il provisioning e la gestione dell'hardware del server, del sistema operativo, dello storage e di altri componenti dell'infrastruttura. Tuttavia, la Defense Information Systems Agency (DISA) e i suoi dirigenti incoraggiano la transizione all'IaC per aumentare l'efficienza e migliorare la sicurezza. Se integrato con gli strumenti di virtualizzazione di VMware o cloud commerciali come Amazon Web Services (AWS) o Microsoft Azure, Ansible Automation Platform svolge in automatico il provisioning del server eseguendo il codice con le API esposte.
- **Onboarding di un nuovo membro del team.** Puoi automatizzare l'attività delle applicazioni in risposta agli eventi. In un esempio, il rilevamento di un nuovo membro del team nel sistema di onboarding potrebbe attivare un flusso di lavoro automatizzato per creare account sui sistemi hardware e software appropriati. Al contrario, quando una persona lascia un team, Ansible Automation Platform potrebbe archiviare o rimuovere automaticamente l'accesso ai suoi account. Allo stesso modo, l'aggiunta di un nuovo endpoint applicativo potrebbe attivare un flusso di lavoro automatizzato per richiamare le regole del firewall, attivare la scansione di sicurezza o notificare ai team la disponibilità di un servizio.

I vantaggi di Red Hat Ansible Automation Platform per le SOF

Ansible Automation Platform è efficace e semplice da adottare perché:

- **Offre l'accreditamento di sicurezza.** Ulteriori informazioni sulla STIG (Security Technical Implementation Guide) per l'Automation Controller in Red Hat Ansible Automation Platform sono disponibili in Ansible Content Collections.
- **Richiede formazione o riaddestramento minimi.** Ansible Automation Platform è già utilizzato dai team delle SOF di tutto il mondo, il che ne semplifica l'adozione.
- **È indipendente dai fornitori.** Utilizza Ansible Automation Platform per automatizzare la configurazione e l'applicazione di patch a una risorsa. Integra le procedure dall'ambiente core all'edge tattico.

- **Integra gli strumenti esistenti.** Anziché sostituire gli strumenti di automazione esistenti e specifici per i prodotti in uso, Ansible Automation Platform li riunisce in una sola piattaforma, aumentandone il valore. Ad esempio, i team che utilizzano Hashicorp Terraform per IaC possono richiamare i flussi di lavoro Terraform da Ansible Automation Platform, la stessa interfaccia che utilizzano per altre attività automatizzate.

Automatizza le attività di routine per accelerare la modernizzazione delle SOF

L'automazione della configurazione e dell'applicazione delle patch è un'azione semplice che ha effetti duraturi sulle operazioni IT. Con Red Hat Ansible Automation Platform, le SOF sono in grado di gestire un ambiente IT più ampio con lo stesso personale, soddisfare le richieste di risorse in meno tempo, rafforzare il profilo di sicurezza e dare al personale più tempo da dedicare a iniziative ad alto valore come MDO e framework zero trust.

Scopri di più

Red Hat collabora con le forze operative speciali per fornire soluzioni di importanza critica. Contatta un rappresentante di Red Hat per maggiori informazioni.

Informazioni su Red Hat

Red Hat consente la standardizzazione in diversi ambienti e lo sviluppo di applicazioni cloud native, oltre a favorire l'integrazione, l'automazione, la protezione e la gestione di ambienti complessi grazie a pluripremiati servizi di consulenza, formazione e supporto.

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
#3134372_1225