

Eventi di sicurezza basati su Webhook are not Received at the On-Prem HTTP Connector for SIEM Integration

Sommario

Problema

Eventi di protezione basati su Webhook non ricevuti nel connettore HTTP locale per l'integrazione SIEM.

Ambiente

- Prodotto: Cisco Secure Access (SSE)
- Tecnologia: supporto della soluzione - creazione di rapporti e registrazione ad accesso sicuro
- Tipo di integrazione: integrazione di terze parti basata su Webhook
- Connettore di destinazione: connettore HTTP locale
- Stato dashboard: caricamento delle integrazioni di terze parti completato in Amministrazione > Integrazioni di terze parti

Risoluzione

Per risolvere i problemi di recapito dei webhook con integrazioni di terze parti Cisco Secure Access, configurare le regole del firewall in modo da consentire il traffico HTTPS in entrata da questi intervalli IP di origine SSE di Cisco.

Configurazione necessaria del firewall

Consenti il traffico HTTPS in entrata da questi intervalli IP di origine SSE Cisco al connettore locale:

146.112.161.0/24

146.112.163.0/24

146.112.165.0/24

146.112.167.0/24

Questi intervalli IP rappresentano gli indirizzi IP condivisi utilizzati da Cisco SSE nelle regioni

dell'UE e degli USA per la consegna del webhook.

Fasi di verifica

Passaggio 1: verificare lo stato di integrazione di terze parti nel dashboard SSE.

Passare a Amministrazione > Integrazioni di terze parti nel dashboard SSE e verificare che le integrazioni vengano caricate correttamente per l'organizzazione.

Passaggio 2: Configurare le regole del firewall.

Aggiornare il firewall di rete e gli eventuali firewall in ingresso per consentire le connessioni HTTPS in ingresso dagli intervalli IP SSE specificati al server del connettore locale.

Passaggio 3: Monitorare il recapito degli eventi webhook.

Dopo aver implementato le modifiche del firewall, monitorare il connettore HTTP locale per verificare che gli eventi webhook vengano ricevuti da Cisco SSE.

Risoluzione dei problemi aggiuntivi

Se gli eventi webhook non vengono ancora ricevuti dopo la configurazione delle regole firewall:

- Verificare che il connettore locale sia configurato correttamente e in ascolto sulla porta prevista.
- Verificare la connettività di rete tra gli indirizzi IP di origine SSE e l'endpoint del connettore.
- Esaminare la configurazione dell'integrazione webhook nel dashboard SSE.
- È consigliabile pianificare una sessione di risoluzione dei problemi in tempo reale per esaminare la consegna del webhook in tempo reale.

Causa

L'errore di recapito del webhook si verifica quando i firewall di rete bloccano le connessioni HTTPS in entrata dagli indirizzi IP di origine SSE di Cisco al connettore HTTP locale. Cisco SSE utilizza intervalli IP specifici di infrastrutture condivise nelle regioni dell'UE e degli USA per fornire eventi webhook, che devono essere esplicitamente consentiti tramite configurazioni firewall per la corretta trasmissione degli eventi.

Contenuto correlato

- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).