Webhook-based Security Events are not Received at On-prem HTTP Connector for SIEM-integratie

Inhoud

uitgeven

Webhook-gebaseerde beveiligingsevenementen worden niet ontvangen in de on-premises HTTP-connector voor SIEM-integratie.

milieu

- Cisco Secure Access (SSE)
- Technologie: Oplossingsondersteuning - Veilige toegangsrapportage en -registratie
- Integratietype: integratie van derden via webhook
- Doelconnector: on-premises HTTP-connector
- Dashboardstatus: integraties van derden worden succesvol geladen in Beheer > Integraties van derden

resolutie

Als u problemen met de levering van webhook wilt oplossen met Cisco Secure Access-integraties van derden, configureert u firewallregels om inkomende HTTPS-verkeer vanuit deze Cisco SSE-bron-IP-bereiken toe te staan.

Vereiste firewallconfiguratie

Sta inkomend HTTPS-verkeer toe van deze Cisco SSE-bron-IP-bereiken naar uw on-premises connector:

```
146.112.161.0/24

146.112.163.0/24

146.112.165.0/24

146.112.167.0/24
```

Deze IP-bereiken vertegenwoordigen de gedeelde IP-adressen die door Cisco SSE uit zowel de EU- als de VS-regio's worden gebruikt voor de levering van webhook.

Verificatiestappen

Stap 1: Controleer de integratiestatus van derden in het SSE-dashboard.

Navigeer naar Beheer > Integraties van derden in uw SSE-dashboard en bevestig dat integraties correct worden geladen voor uw organisatie.

Stap 2: Firewallregels configureren.

Werk uw netwerkfirewall en eventuele tussenliggende firewalls bij om inkomende HTTPS-verbindingen mogelijk te maken van de verstrekte SSE IP-bereiken naar uw on-premises connectorserver.

Stap 3: Controleer de levering van webhook-evenementen.

Nadat u de firewallwijzigingen hebt geïmplementeerd, controleert u uw on-premises HTTP-connector om te controleren of webhook-gebeurtenissen worden ontvangen van Cisco SSE.

Extra probleemoplossing

Als er na het configureren van de firewallregels nog steeds geen webhook-gebeurtenissen worden ontvangen:

- Controleer of de on-premises connector correct is geconfigureerd en luister naar de verwachte poort.
- Controleer de netwerkconnectiviteit tussen de SSE-bron-IP's en het connectoreindpunt.
- Controleer de configuratie van de webhook-integratie in het SSE-dashboard.
- Overweeg een live probleemoplossingssessie in te plannen om de levering van de webhook in realtime te beoordelen.

Oorzaak

De leveringsfout van de webhook treedt op wanneer netwerkfirewalls inkomende HTTPS-verbindingen van Cisco SSE-bron-IP-adressen naar de on-premises HTTP-connector blokkeren. Cisco SSE maakt gebruik van specifieke IP-bereiken van gedeelde infrastructuur in de EU en de VS regio's om webhook evenementen te leveren, en deze moeten expliciet worden toegestaan via firewall configuraties voor succesvolle event delivery.

Verwante inhoud

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.