Hook-basierte Sicherheitsereignisse are not Received at the On-Prem HTTP Connector für SIEM-Integration

Inhalt

Problem

Webhook-basierte Sicherheitsereignisse werden zur SIEM-Integration nicht am lokalen HTTP-Connector empfangen.

Umwelt

- Produkt: Cisco Secure Access (SSE)
- Technologie: Lösungssupport - Berichte und Protokolle für sicheren Zugriff
- Integrationstyp: webhook-basierte Drittanbieterintegration
- Zielkonnektor: Lokaler HTTP-Konnektor
- Dashboard-Status: Integration von Drittanbietern wird erfolgreich geladen unter Admin > Integration von Drittanbietern

Auflösung

Konfigurieren Sie Firewall-Regeln, um eingehenden HTTPS-Datenverkehr aus diesen Cisco SSE-Quell-IP-Bereichen zuzulassen, um Probleme bei der Übertragung über Webhook mit Cisco Secure Access zu beheben, das in Drittanbieterlösungen integriert ist.

Erforderliche Firewall-Konfiguration

Zulassen des eingehenden HTTPS-Datenverkehrs von den folgenden Cisco SSE-Quell-IP-Bereichen zu Ihrem Connector am Standort:

```
146.112.161.0/24

146.112.163.0/24

146.112.165.0/24

146.112.167.0/24
```

Diese IP-Bereiche stellen die gemeinsam genutzten IP-Adressen dar, die von der Cisco SSE für die Webhook-Übermittlung aus der EU und den USA verwendet werden.

Verifizierungsschritte

Schritt 1: Überprüfen des Integrationsstatus von Drittanbietern im SSE Dashboard

Navigieren Sie in Ihrem SSE-Dashboard zu Admin > Third Party Integrations (Admin > Integration von Drittanbietern), und stellen Sie sicher, dass die Integration für Ihr Unternehmen korrekt geladen wird.

Schritt 2: Konfigurieren von Firewall-Regeln

Aktualisieren Sie Ihre Netzwerk-Firewall und alle dazwischenliegenden Firewalls, um eingehende HTTPS-Verbindungen von den bereitgestellten SSE-IP-Bereichen zum Connector-Server vor Ort zuzulassen.

Schritt 3: Überwachen der Übertragung von Webhook-Ereignissen

Nachdem Sie die Änderungen an der Firewall implementiert haben, überwachen Sie den lokalen HTTP-Connector, um sicherzustellen, dass Webhook-Ereignisse von der Cisco SSE empfangen werden.

Zusätzliche Fehlerbehebung

Wenn Webhook-Ereignisse nach der Konfiguration der Firewall-Regeln immer noch nicht empfangen werden:

- Überprüfen Sie, ob der lokale Anschluss richtig konfiguriert ist und den erwarteten Port abhört.
- Überprüfen Sie die Netzwerkverbindung zwischen den SSE-Quell-IPs und dem Connector-Endpunkt.
- Überprüfen der Konfiguration der Webhook-Integration im SSE Dashboard
- Planen Sie eine Live-Sitzung zur Fehlerbehebung ein, um die Webhook-Bereitstellung in Echtzeit zu überprüfen.

Ursache

Der Fehler bei der Übermittlung über den Webhook tritt auf, wenn Netzwerk-Firewalls eingehende HTTPS-Verbindungen von den Cisco SSE-Quell-IP-Adressen zum lokalen HTTP-Connector blockieren. Cisco SSE nutzt für die Bereitstellung von Webhook-Events spezifische IP-Bereiche aus gemeinsam genutzten Infrastrukturen in der EU und den USA. Diese müssen explizit über Firewall-Konfigurationen zugelassen werden, damit die Veranstaltung erfolgreich durchgeführt werden kann.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.