基於Webhook的安全事件 ；是 ；不是 ；已接收 at ；內部HTTP聯結器 ；用於 SIEM整合

目錄

問題

在用於SIEM整合的本地HTTP聯結器上未收到基於Webhook的安全事件。

環境

- 產品：思科安全訪問(SSE)
- 技術：解決方案支援 — 安全訪問報告和記錄
- 整合型別：基於Webhook的第三方整合
- 目標聯結器：本地HTTP聯結器
- 控制面板狀態：在「管理」>「第三方整合」中成功載入第三方整合

解析

要解決Cisco Secure Access第三方整合的webhook交付問題，請配置防火牆規則以允許來自這些Cisco SSE源IP範圍的入站HTTPS流量。

所需的防火牆配置

允許從這些Cisco SSE源IP範圍到本地聯結器的入站HTTPS流量：

```
146.112.161.0/24

146.112.163.0/24

146.112.165.0/24

146.112.167.0/24
```

這些IP範圍代表歐盟和美國的Cisco SSE用於Webhook交付的共用IP地址。

驗證步驟

第1步：在SSE控制面板中驗證第三方整合狀態。

在SSE控制面板中導航到Admin > Third Party Integrations，並確認已為您的組織正確載入整合。

第2步：配置防火牆規則。

更新網路防火牆和任何介入防火牆，以允許從提供的SSE IP範圍到本地聯結器伺服器的入站HTTPS連線。

第3步：監控webhook事件傳遞。

實施防火牆更改後，監控本地HTTP聯結器，以驗證是否正在從Cisco SSE接收Webhook事件。

其他疑難排解

如果在配置防火牆規則後仍未收到webhook事件：

- 驗證內部部署聯結器是否配置正確並在預期埠上偵聽。
- 檢查SSE源IP和聯結器端點之間的網路連線。
- 檢視SSE控制面板中的Webhook整合配置。
- 考慮安排即時故障排除會話，以即時檢視webhook交付。

原因

當網路防火牆阻止從思科SSE源IP地址到本地HTTP聯結器的入站HTTPS連線時，就會發生Webhook傳遞失敗。Cisco SSE使用來自歐盟和美國地區的共用基礎設施的特定IP範圍來傳送Webhook事件，這些事件必須通過防火牆配置明確允許才能成功傳送。

相關內容

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。