配置安全訪問Webhook整合的IP範圍和防火牆

問題

第三方整合在Cisco Secure Access(SSE)控制面板中成功載入，但在用於SIEM整合的本地HTTP聯結器上未收到基於Webhook的安全事件。組織要求明確思科SSE源IP範圍（包括區域特定的IP），以正確配置防火牆規則並啟用webhook事件交付。

環境

- 產品:思科安全存取(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聯結器伺服器

解析

要解決思科安全訪問整合的webhook傳遞問題，請配置防火牆規則以允許從指定SSE源IP範圍到本地聯結器的入站HTTPS流量。

Cisco SSE來源IP範圍

將防火牆配置為允許來自以下Cisco SSE源IP範圍的入站HTTPS連線：

```
146.112.161.0/24
146.112.163.0/24
146.112.165.0/24
146.112.167.0/24
```

防火牆配置步驟

步驟 1: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。

步驟 2:配置防火牆規則

建立防火牆規則以允許從SSE源IP範圍到您的本地聯結器伺服器的入站HTTPS流量（埠443）。確保將規則應用於您的網路防火牆以及Internet和聯結器伺服器之間的任何介入防火牆。

步驟 3:驗證Webhook事件傳遞

實施防火牆更改後，監控本地HTTP聯結器，以確認正在從Cisco SSE接收Webhook事件。

地區IP資訊

Cisco SSE僅使用來自歐盟和美國地區的共用IP範圍。提供的IP範圍涵蓋這兩種區域部署，無論您的組織位於哪個主要區域，都必須進行配置。

原因

來自Cisco Secure Access的Webhook事件被防火牆規則阻止，這些規則不允許從SSE源IP地址到本地HTTP聯結器伺服器的入站HTTPS連線。當SSE控制面板顯示成功整合載入時，實際的webhook交付需要特定的防火牆配置以允許來自思科基礎設施的流量到達使用者聯結器端點。

相關內容

- 思科安全存取檔案
- 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）。