

Secure Access Activity Search顯示 UNKNOWN規則名稱

目錄

問題

在Umbrella到SSE遷移期間，安全訪問活動搜尋事件將規則名稱顯示為UNKNOWN，而不是顯示命名策略規則。針對各種流量型別(包括允許的流量，例如對chatgpt.com的請求)觀察到此行為。問題在於這些UNKNOWN規則名稱條目是否指示需要修復的策略配置問題或遷移問題。

環境

- 思科安全存取(SSE)
- 正在從Umbrella遷移到SSE的組織
- 安全訪問活動搜尋報告
- 分類為新發現的域的流量

解析

對於Secure Access系統邏輯處理的事件（而不是客戶建立/命名的規則），應該是Rule Name UNKNOWN行為，並且是正常行為。這種情況通常發生在歸類為「新發現的域」的流量中，該域在查詢時是新發現的，並在「活動搜尋」或「安全活動」報告中按原樣報告。

使用未知規則名稱解釋活動搜尋事件

遇到規則名稱為UNKNOWN的事件時，請檢視這些事件欄位以確定實施原因並確認正確的策略應用：

- Action — 顯示流量是被允許還是被阻止
- 事件阻止原因/阻止原因 — 提供具體的實施詳細資訊
- 類別 — 顯示內容分類(例如新看見的域)
- 目標域/IP — 請求的目標
- 使用者/源身份 — 流量的來源
- Timestamp — 事件發生時間

如果Categories欄位顯示Newly Seen Domains，則規則名稱欄位中的UNKNOWN是預期行為，並不表示遷移失敗或策略損壞。

意外行為的驗證步驟

如果流量應該與特定命名規則匹配，但顯示UNKNOWN，請收集此資訊以進行策略路徑驗證：

- 2-3個示例事件時間戳
- 每個事件的目標域/IP
- 每個事件的使用者/源標識

此資訊可用於比較預期策略路徑與實際事件行為，並確定是否需要進一步調查。

原因

當Secure Access系統邏輯處理流量，而不是應用客戶建立/命名的策略規則時，會顯示UNKNOWN規則名稱。這是某些流量類別（尤其是新發現的域）的已記錄行為，在初始域評估期間，內建分類和處理機制優先於命名規則。

相關內容

- [啟用新看見的域安全](#)
- [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）。