許可證更改後SIEM中缺少安全訪問檔案事件日誌

目錄

問題

SIEM從AWS S3儲存中停止接收檔案事件日誌，而DNS日誌繼續成功傳送。檔案事件資料聯結器在SIEM介面中顯示了一個「斷開連線」圖示。停止顯示的日誌被標識為DLP/IPS相關的檔案事件記錄。DNS層日誌在整個問題期間保持正常運行。

遷移期間，環境同時使用Umbrella和安全訪問，並將日誌傳送到同一個AWS儲存桶。鑰匙已輪換，並已確認工作正常。模式版本被注意到是版本10，而版本16可用。

環境

- 思科安全訪問組織，具有Umbrella和安全訪問配置
- 用於日誌匯出的AWS S3儲存整合
- Microsoft Sentinel SIEM平台
- 使用的架構版本10（版本16可用）
- 2026年6月23日，安全訪問許可證從Advantage更改為Essentials
- 上次觀察到的檔案事件日誌為2026年6月24日

解析

調查發現，檔案事件日誌與DLP/IPS功能相關，而後者需要特定的許可功能。通過下一個分析確定了根本原因。

步驟 1:流量分析

檢查安全訪問中的活動搜尋以確認流量模式：

1. — 導航到活動搜尋，然後過濾網路流量或惡意處置事件。分析顯示存在DNS流量，但過去30天內未顯示任何Web流量事件，並且未標識啟用了檔案檢查的規則。
2.- Traffic Flow > Logs on the CSA report > S3 bucket - SIEM。

步驟 2:許可證歷史記錄稽核

1. — 檢視Secure Access中的許可證歷史記錄，以確定與檔案事件日誌停止時間一致的任何更改。

2. — 導航到Secure Access > Admin > Subscription以檢視當前許可證級別和功能摘要。

調查顯示，2026年6月23日，安全訪問許可證從Secure Access Advantage更改為Secure Access Essentials，與檔案事件日誌停止出現的時間一致。

步驟 3:功能驗證

驗證當前許可證級別中包括哪些功能。DLP和IPS功能會生成檔案事件日誌，但不包含在Secure Access Essentials許可證層中。

步驟 4:確認和根本原因

當檔案事件日誌停止顯示時，許可證更改的時間完全匹配。由於DNS層日誌記錄仍然正常工作並且是主要要求，因此解決此案例時已認識到檔案事件日誌在當前的Essentials許可證下不可用。

原因

2026年6月23日，由於許可證從Secure Access Advantage更改為Secure Access Essentials，檔案事件日誌停止生成。檔案事件日誌與DLP和IPS功能相關聯，而Essentials許可證層不包含這些功能。許可證降級刪除了對生成這些特定日誌型別的檔案檢查功能的訪問。

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）。