

通過日誌匯出或報告API瞭解資料管理

目錄

- [簡介](#)
- [必要條件](#)
 - [需求](#)
 - [採用元件](#)
- [概觀](#)
- [其他資訊](#)

簡介

本檔案介紹如何使用Cisco Umbrella中的日誌匯出或報告API管理資料。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco Umbrella。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

Umbrella是一個功能強大的工具，可為您提供大量有關網際網路流量的資訊。以下是一個簡單的指南，可以幫助您確定如何最好地使用資料：

使用案例	粒度/型別	建議	注意事項
法規遵從性/長期事件保留	匯出並儲存所有事件	S3:客戶擁有的儲存桶	可以使用Cisco Managed Bucket，但資訊最多只能保留30天。
SIEM:事件關聯	匯出所有事件	S3:思科管理的儲存桶	資訊的保留期不超過30天；需要處理解除安裝。
儀表板KPI/構件	活動搜尋/聚合	報告API	必須最佳化查詢，因為寬查詢可能會導致超時。

生成報告	聚合	報告API	
SOAR工作流：觸發	活動搜尋	報告API	必須最佳化查詢，因為寬查詢可能會導致超時。

其他資訊

- 有關如何管理日誌的說明：[Umbrella文檔 — 管理您的日誌](#)
- 有關如何管理API的說明：[Cisco DevNet-Cisco雲安全API](#)

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）。