為S3儲存段的HTTPS事務配置日誌查詢字串引數

目錄

簡介

本文檔介紹了要記錄到s3儲存桶的HTTPS事務的新日誌查詢引數。

概觀

現在有新的日誌記錄功能，可以將包括查詢字串引數的完整HTTPS請求記錄到s3儲存桶。

預設情況下，在將詳細資訊記錄到Umbrella的報告和S3儲存段之前，Umbrella從所有HTTPS請求中刪除查詢字串引數。這樣做是為了防止在任何報告中不小心地暴露查詢引數，因為這些引數可能包含私人或敏感資訊。

s3儲存桶通常用於向SIEM和專家報告工具提供活動資料。通過為HTTPS事務啟用日誌查詢引數，這些工具可以對HTTPS請求獲得更多的可視性和見解。

1. HTTPS流量（已加密）和查詢字串引數繼續從Umbrella報告控制面板中刪除。
2. 對於HTTP流量（非加密），Umbrella始終記錄包含查詢字串引數的完整URL。HTTP流量的引數不被認為是「敏感」的，因為應用/網站不對其進行加密。

有關如何啟用此新的s3儲存桶日誌記錄功能的更多詳細資訊，請參閱Umbrella文檔。

- 啟用記錄到您自己的S3儲存桶 — https://docs.umbrella.com/umbrella-user-guide/docs/enable-logging-to-your-own-s3-bucket
- 啟用登入到思科管理的S3儲存桶 — https://docs.umbrella.com/umbrella-user-guide/docs/enable-logging-to-a-cisco-managed-s3-bucket

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）。