解決思科安全訪問的即時DLP問題

目錄

介紹

本檔案介紹在安全Web閘道(SWG)環境中進行內嵌或即時資料遺失防範(DLP)問題的疑難排解步驟。

先決條件和警告

- HTTPS檢查：確保啟用HTTPS檢查。DLP無法掃描加密流量。確保網站已使用思科安全訪問根CA或自定義CA解密。
- QUIC協定：在所有瀏覽器中禁用QUIC協定。QUIC使用UDP，它繞過SWG並阻止DLP掃描。
- IPv6:如果流量未達到SWG，則禁用IPv6，因為雙堆疊功能必須導致繞過。
- 安全策略：確保訪問規則未啟用「允許 — 覆蓋安全」或「隔離」。

概觀

內聯DLP是SWG的擴展掃描功能。它會監視或阻止通過SWG代理上傳的檔案中的敏感、機密或個人身份資料的上傳。客戶使用思科定義的識別符號（例如信用卡或社會保險號碼）或自定義關鍵字建立資料分類。這些分類適用於分配給特定標識和目標的DLP策略。DLP引擎僅掃描HTTP POST、PUT和PATCH方法。

常規故障排除核對表

如果未進行DLP檢測，請驗證所概述的步驟：

- 連線：通過訪問http://policy.test.sse.cisco.com確認客戶端正在使用SWG。驗證應用了正確的SWG資料中心，測試結果顯示為「受安全訪問保護」。
- 解密：確保在安全配置檔案中啟用SSL解密。驗證沒有選擇性解密或「不解密」清單排除。
- Traffic Steering:確保在「Internet設定」中未配置外部域繞行。
- 身份：如果DLP策略依賴於Active Directory組，請確認該使用者是正確組的成員。
- 應用程式設定：如果正在將Microsoft域用於DLP，請確保禁用了Office 365旁路或M365相容性設定。
- 活動搜尋：使用Reporting > Activity Search確保完整URL可見（已解密），並且預期標識與流量相關聯。選中Reporting > Data Loss Prevention，確認是否記錄監控程式或阻止活動。
- 策略配置：驗證DLP策略是否針對正確的身份和目標應用程式進行了配置。
- 測試：使用確認完好的目的地(例如pastebin.com或dlptest.com)和來自Cisco文檔的確認完好的測試字串示例。
- 支援資料：從使用者處收集HAR檔案，以驗證流量是否通過SWG路由並檢查SWG報頭。

排除漏報故障

如果DLP處於活動狀態，但特定分類器無法觸發，請調查以下區域：

分類器、檔案和字串

- 檔案狀態：確保檔案未加密或不可掃描。使用簡單文本檔案測試。
- 閾值：檢查Policy > Data Classification中的Threshold和Proximity設定。分類器可能需要較高的命中數或接近自定義字串。
- Regex模式：使用線上工具(例如regexr.com)視覺化模式。簡化模式以捕獲更小部分字串並逐漸擴展。

檔案標籤

- 相容性：檔案標籤檢測對Confluence或JIRA不起作用。
- 後設資料：在Microsoft應用程式中開啟文檔屬性。該值必須與Umbrella File標籤完全匹配；區分大小寫。
- 加密:標籤檢測不適用於受密碼保護或加密的檔案。

網站和目標

- 支援的應用：檢視支援的應用程式清單。對於不受支援的應用或「所有目標」，僅掃描特定的mime型別。
- 經過稽核的應用程式：對經過稽核的應用程式(例如dlptest.com)進行更全面的掃描。只能掃描任意網站是否存在檔案違規。
- 檔名：系統僅為某些經過稽核的應用程式搜尋檔名。

排除誤報故障

如果DLP意外匹配內容，請在Reporting > Data Loss Prevention中檢查分類器名稱和DLP規則。如果檢測是合法的，但不需要檢測，請調整「閾值」或「接近」設定以最佳化策略。

案頭應用程式支援

對基於案頭的應用程式（例如Outlook、Teams或Google Workspace）的支援是以盡力為基礎的。有效性取決於檔案上傳過程中使用的消息格式，基於Web的版本與案頭版本之間可能有所不同。對於未經稽核的應用程式，無法保證支援檔案上傳。

DLP分類器漏洞

- 信用卡號：使用Luhn演算法進行驗證。僅使用有效的信用卡號進行測試。
- 人員姓名：需要2-3個單詞，並且每個單詞必須大寫。
- 名稱組合：名稱和其他資料之間需要分隔符字串（例如，「Viagra - John Smith」匹配，但「Viagra John Smith」不匹配）。
- 出生日期：必須靠近關鍵字或標題，如「dob」或「出生日期」。
- 令人反感的內容：如果文本類似於書籍或報告，某些異常字串會阻止此分類器觸發。
- 郵遞區號：必須鄰近特定的位置相關關鍵字。

精確資料匹配(EDM)

在研究EDM之前，請確認常規DLP掃描是否工作正常。針對EDM特定的問題，請檢查「上次編輯」(Last Edit)欄位是否在儀表板中是當前欄位，並驗證索引工具輸出。

命令用法：

使用-d選項運行索引工具，以生成布魯姆過濾器檔案(.blm)。 此命令用於驗證EDM索引和排除必須跳過記錄的原因。-d標誌指示工具輸出診斷布盧姆過濾器檔案，該檔案應與支援人員共用以及示例檔案或HAR/Web開發人員工具資料。

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）。