使用DLP監控AWS S3和Azure儲存中的敏感資料暴露

目錄

簡介

本文檔介紹如何使用資料丟失防護(DLP)監控AWS S3和Azure儲存中的敏感資料洩露。

概觀

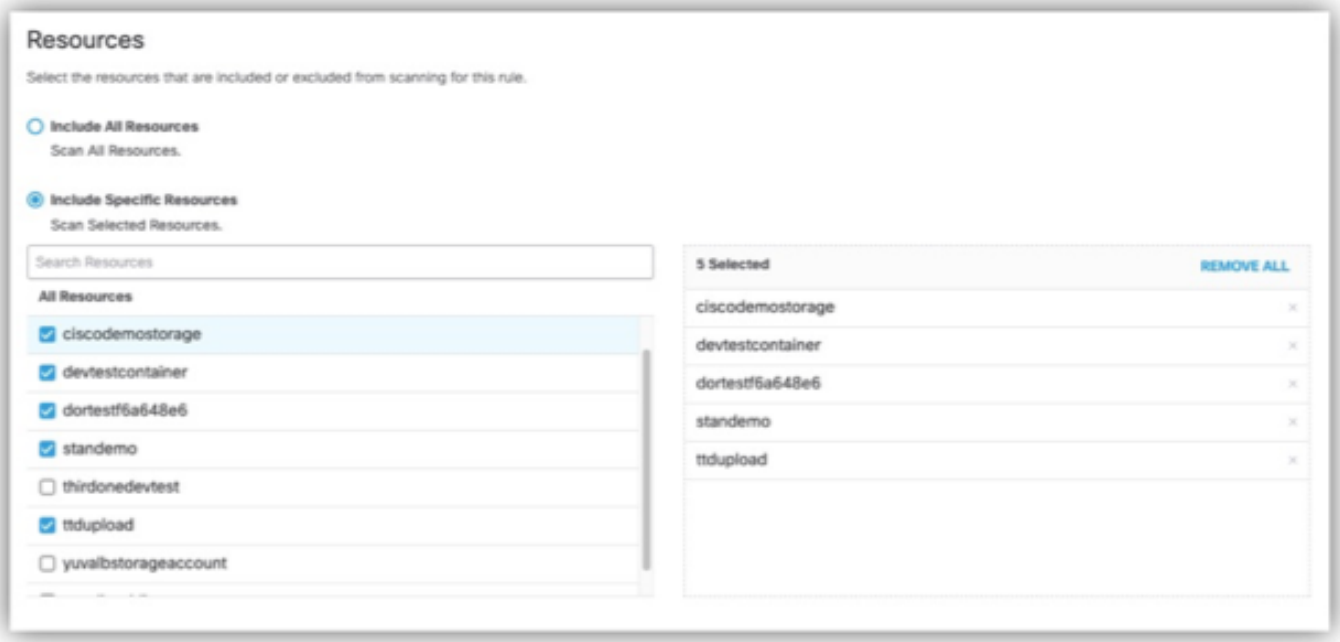
有了適用於AWS S3和Azure儲存的新聯結器，您現在可以在雲環境中掃描敏感資料暴露。這些功能可幫助您發現並監控暴露的憑據（如API金鑰、機密和令牌）以及敏感資料(包括可能暴露於公共Web中的個人識別資訊(PII)、財務記錄和醫療保健資訊)。

在AWS S3和Azure檔案儲存中掃描哪些內容？

- AWS S3:
  DLP對預先存在的敏感資料執行初始發現掃描，並對新檔案或更新檔案執行持續監控。您可以通過在DLP規則中選擇要掃描的S3儲存桶。

- Azure檔案儲存：
  DLP支援新檔案或更新檔案的初始發現和持續監控。你可以選擇要在DLP規則內掃描的特定Azure容器。

您可以通過選擇準確的AWS S3儲存桶或Azure容器來定製DLP掃描，以滿足您的需求和優先順序。



AWS和Azure支援的響應操作

目前，僅支援將監控作為AWS S3和Azure儲存的響應操作。自動補救操作（如檔案刪除或隔離）不可用。此方法避免了中斷任務關鍵型IaaS環境的風險，同時仍使您能夠高效地監控敏感資料的洩露。

查詢AWS S3儲存桶和Azure儲存Blob以進行手動補救

為了協助手動修復，DLP報告包含詳細資訊：

- 該報告顯示實際的S3儲存桶或blob名稱，便於在AWS或Azure控制檯中搜尋。
- 每個DLP違規事件都會提供資源名稱、目標URL以及資源ID（如果可用）。
- 使用此資訊在AWS S3儲存桶和Azure儲存blob中高效地查詢和解決DLP違規。

相關資源

有關詳細指導，請參閱Umbrella文檔：

- 為AWS租戶啟用SaaS API資料丟失保護
- 為Azure租戶啟用SaaS API資料丟失保護
- 將SaaS API規則新增到資料丟失防護策略
- 防資料丟失報告

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）。