在Slack和ServiceNow中為SaaS API DLP啟用和配置自動補救

目錄

簡介

本文檔介紹如何為Slack和ServiceNow租戶中的SaaS API DLP啟用和配置自動補救。

概觀

現在，您可以發現並自動修復Slack和ServiceNow租戶中的敏感資料洩露。這有助於保持合規性並防止敏感資料（如智慧財產權或其他系統的憑證）被洩露。

為受支援的平台授權新租戶

作為管理員，您可以使用Umbrella控制面板中的SaaS API資料丟失防護(DLP)功能對Slack和ServiceNow的新租戶進行身份驗證。

1. 在Umbrella控制面板中轉至ADMIN > AUTHENTICATION > PLATFORMS。
2. 根據提示對新租戶進行身份驗證。

SaaS API DLP支援的自動補救

- ServiceNow:
  SaaS API DLP支援自動隔離。隔離的檔案儲存在思科隔離表中。只有對租戶進行身份驗證的管理員才能訪問此表。

- Slack:
  SaaS API DLP支援自動刪除檔案和消息。

為受感染的檔案配置自動補救

作為管理員，您可以配置SaaS API DLP以自動修正敏感資料洩露。

在SaaS API DLP規則中設定響應操作：

1. 在Umbrella控制面板中，轉至POLICIES > MANAGEMENT > DATA LOSS PREVENTION POLICY。
2. 按一下ADD RULE。
3. 選擇SAAS API規則。

4. 在「響應操作」部分設定desiredACTION以啟用自動補救。

尋找詳細資訊

請參閱Umbrella文檔以獲取詳細指導。

- 為Slack租戶啟用SaaS API資料丟失保護
- 為ServiceNow租戶啟用SaaS API資料丟失保護

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）。