為Slack和ServiceNow中的雲惡意軟體配置自動補救

目錄

簡介

本文檔介紹如何為Slack和ServiceNow租戶中的雲惡意軟體啟用和配置自動補救。

概觀

現在，您可以發現並自動修正Slack和ServiceNow租戶中的惡意軟體風險。這些功能通過刪除或隔離感染病毒的檔案幫助保護租戶的安全。

為受支援的平台授權新租戶

作為管理員，您可以通過Umbrella控制面板對雲惡意軟體防護的新Slack或ServiceNow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。

雲惡意軟體支援的自動補救

- ServiceNow:
  雲惡意軟體支援自動隔離。隔離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。

- Slack:
  雲惡意軟體支援自動刪除受感染檔案。

為受感染的檔案配置自動補救

作為管理員，您可以配置Cloud Malware以自動修正感染病毒的檔案：

1. 在Umbrella控制面板中，轉至ADMIN > AUTHENTICATION > PLATFORMS。
2. 使用租戶的身份驗證嚮導。在步驟3中設定響應操作。
3. 選擇您的首選響應操作（隔離或監控）。
4. 您可以根據需求變化隨時更新響應操作。

相關資源

- 為Slack租戶啟用雲惡意軟體保護
- 為ServiceNow租戶啟用雲惡意軟體保護

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）。