使用雲惡意軟體監控AWS S3和Azure儲存中的惡意軟體風險

目錄

簡介

本文檔介紹如何監控和解決帶有雲惡意軟體的AWS S3和Azure儲存中的惡意軟體風險。

概觀

藉助此功能，您現在可以發現並監控AWS S3和Azure儲存環境中的惡意軟體風險。一個關鍵的使用案例是識別被惡意軟體感染的檔案，這些檔案可能會竊取憑據或利用漏洞，從而增加在您的環境中橫向移動或在其他環境中橫向移動的風險。

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。此限制可防止任務關鍵型服務意外中斷，同時仍允許您監控敏感資料洩露和惡意軟體風險。

相關資源

- 為AWS租戶啟用雲惡意軟體保護
- 為Azure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）。