安全訪問安全配置檔案對警告操作的解密要求

目錄

問題

使用者需要思科安全訪問的配置指南，內容涉及當訪問策略操作設定為警告時，是否必須在安全配置檔案設定中啟用解密。特定問題適用於以下安全配置檔案功能：

- 威脅類別
- 檔案檢查
- Cisco Secure 惡意軟體分析
- 檔案型別阻止
- 安全搜尋

問題的中心是瞭解訪問策略警告操作和安全配置檔案解密要求之間的關係，以便這些安全功能正常運行。

環境

- 產品:思科安全網際網路接入優勢
- 技術：安全訪問
- 軟體版本:ALL
- 組態:具有各種安全功能的安全配置檔案
- 策略配置：具有警告操作設定的訪問策略

解析

實驗室驗證確認，即使在安全配置檔案中僅啟用解密，並且禁用所有其他功能，訪問策略警告操作仍能正常工作。這表示對於這些安全配置檔案功能，在使用警告操作時，不需要為每個功能專門啟用解密：

- 威脅類別
- 檔案檢查
- Cisco Secure 惡意軟體分析
- 檔案型別阻止
- 安全搜尋

配置指南

當配置帶有警告操作的訪問策略時：

步驟 1:針對所需的策略規則，將Access Policy（訪問策略）操作配置為Warning（警告）。

步驟 2:在Security Profile設定中，確保在配置檔案級別啟用Decryption。

步驟 3:單個安全功能（威脅類別、檔案檢查、思科安全惡意軟體分析、檔案型別阻止和安全搜尋）可以在其特定的解密設定中保持禁用狀態，同時仍可正常運行警告操作。

此配置方法允許警告操作正常運行，同時保持安全配置檔案功能管理的靈活性。

原因

訪問策略中的Warning（警告）操作與單個安全配置檔案功能解密要求不同。只有在Security Profile級別啟用主解密設定時，Warning操作才能正常工作，而無需對每個特定安全功能啟用單獨解密。

相關內容

- 思科技術支援與下載

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）。