# 在思科安全終端中配置彈出通知

### 目錄

<u>簡介</u> <u>必要條件</u> <u>需採用元件</u> <u>驗</u> 疑難排解

### 簡介

本文檔介紹如何在思科安全終端檢測到惡意檔案時配置彈出通知。

作者:Javier Martinez,思科TAC工程師。

## 必要條件

#### 需求

思科建議您瞭解以下主題:

- 思科安全終端控制檯控制面板
- 具有管理員許可權的帳戶

#### 採用元件

本檔案中的資訊是根據思科安全終端版本6.3.7及更新版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

### 設定

當思科安全終端檢測到、阻止或隔離檔案/進程時,可以在終端中傳送有關主要安全終端的彈出警報 。

步驟1.登入AMP主控台;<u>https://console.amp.cisco.com/</u>,如下圖所示。



步驟2.導覽至Management > Policies (選擇策略) >Advanced settings > Client User Interface。

**引擎通**知功能預設會停用,如下圖所示。

| Modes and Engines              | Start Client User Interface |
|--------------------------------|-----------------------------|
| Exclusions<br>2 exclusion sets | Cloud Notifications         |
| Proxy                          | Hide Exclusions             |
| Outbreak Control               |                             |
| Product Updates                |                             |
| Advanced Settings              |                             |
| Administrative Features        |                             |
| Client User Interface          |                             |
| File and Process Scan          |                             |
| Cache                          |                             |
| Endpoint Isolation             |                             |
| Orbital                        |                             |
| Engines                        |                             |
| TETRA                          |                             |
| Network                        |                             |
| Scheduled Scans                |                             |
| Identity Persistence           |                             |

步驟3.勾選「Engine Notifications」覈取方塊,如下圖所示。



步驟4.若要應用新變更,請導覽至Desktop > OpenCisco Secure Endpoint,然後選擇**Settings**,如 下圖所示。



### 步驟5.按一下Sync Policy,然後選擇OK,如下圖所示。

|  | Settings |
|--|----------|
| *.db-journal<br>*.db-shm<br>*.db-wal<br>*.log<br>*.pst   | ^        |
| Wildcard Excl<br>C:\\Windo<br>C:\\Windo<br>C:\\Windo<br>C:\\Windo<br>C:\\Windo<br>C:\\Windo<br>C:\\Windo |          |
| Scan Settings OK OK  |          |
| Proxy Settings   |          |
| Cisco AMP Connector Settings   | ~        |
| Sync Policy  | Close    |

# 驗證

使用本節內容,確認您的組態是否正常運作。

當安全終端引擎隔離檔案/進程時,您會在案頭上看到彈出通知,如下圖所示。



附註:此配置適用於屬於策略的所有裝置。

# 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

如果安全終結點沒有觸發彈出通知,您可以在安全終結點控制檯上看到警報事件。

導覽至Cisco Secure Endpoint Console > Dashboard > Events,如下圖所示。

| •                 | detected <b>\$RMTWB9L.7z</b> as | Trojan.Agent.DPDW             | Medium         P         P         Quarantine: Successful         2020-09-01 11:18:29 CDT |
|-------------------|---------------------------------|-------------------------------|---|
| File Detection    | Detection                       | Trojan.Agent.DPDW             |   |
| Connector Details | Fingerprint (SHA-256)           | T                             |   |
| Comments          | File Name                       | T \$RMTWB9L.7z                |   |
|                   | File Path                       |                               |   |
|                   | File Size                       | 1.17 KB                       |   |
|                   | Parent                          | No parent SHA/Filename availa | sle,  |
|                   | Analyze 2 Restore File          | 1 All Computers               | ▲ View Upload Status Add to Allowed Applications IP File Trajectory                       |

如果安全終端控制檯中的終端或警報事件中沒有彈出通知,請與思科支援部門聯絡。 思科支援:請訪問<u>http://cisco.com/tac/caseopen</u>或電話:地區免費電話號碼 :http://www.cisco.com/en/US/support/tsd\_cisco\_worldwide\_contacts.html