# 瞭解7.6中的Talos威脅搜尋遙測功能

## 目錄



## 簡介

本檔案將介紹7.6中的Talos威脅搜尋遙測功能。

## 必要條件

### 需求

#### 最低軟體和硬體平台

| Minimum Supported Manager Version | Managed Devices | Min. Supported Managed Device Version Required | Notes |
|---|---|---|---|
| cdFMC/FMC 7.6.0 | FTD in Native Mode/HA/Cluster | • 7.6.0 | Snort 3 only |

- 通過推送到Firepower裝置的特殊規則類，為Talos提供收集情報和誤報測試的能力。
- 這些事件通過SSX聯結器傳送到雲，並且僅由Talos使用。
- 包含威脅搜尋規則的新功能覈取方塊，作為全域性策略配置的一部分。
- 例項 — *目錄中的新日誌檔案(threat_telemetry_snort-unified.log.*)，用於記錄作為威脅搜尋規則一部分生成的入侵事件。
- 將威脅搜尋規則的IPS緩衝區轉儲為額外資料中的新記錄型別。
- EventHandler進程使用新的使用者以完全限定的格式（捆綁和壓縮）將IPS/資料包/外資料事件傳送到雲。
- FMC UI中不顯示這些事件

## 採用元件

本文件所述內容不限於特定軟體和硬體版本。

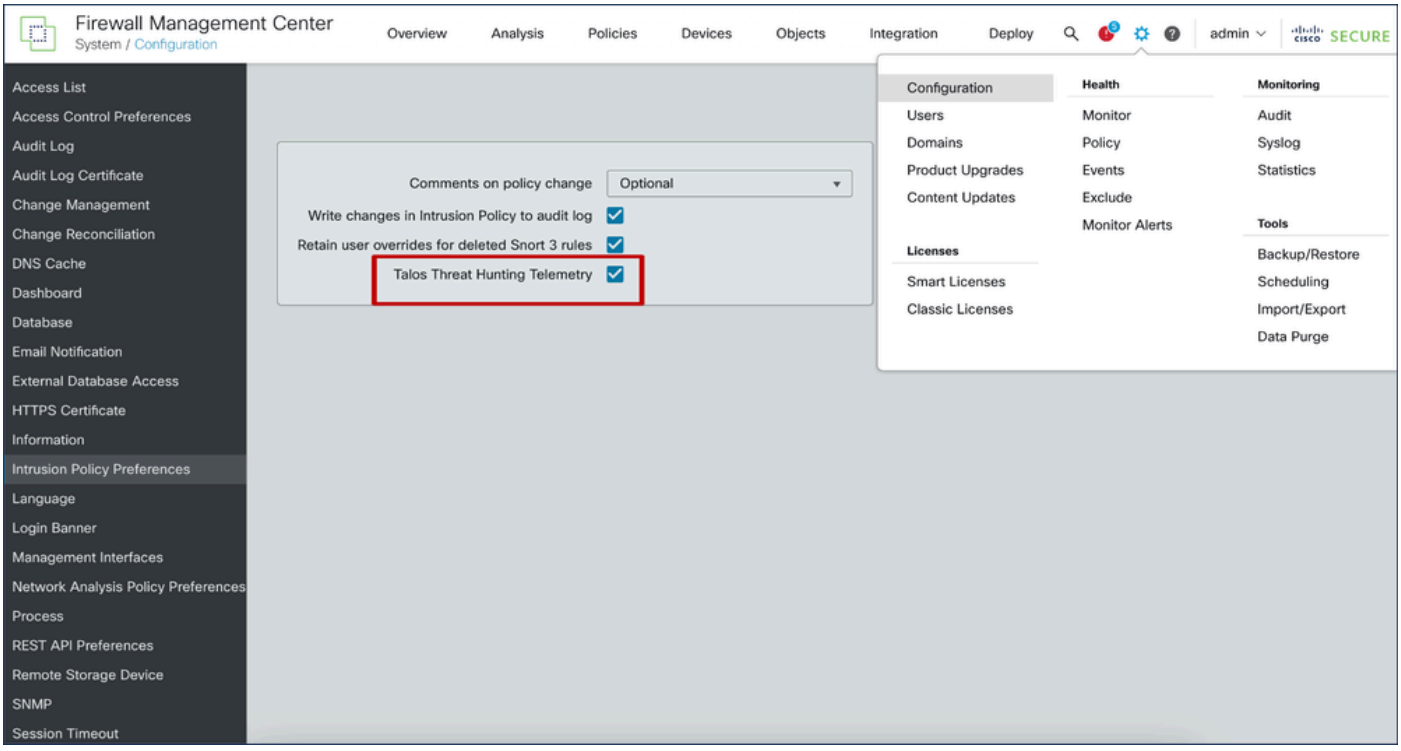
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

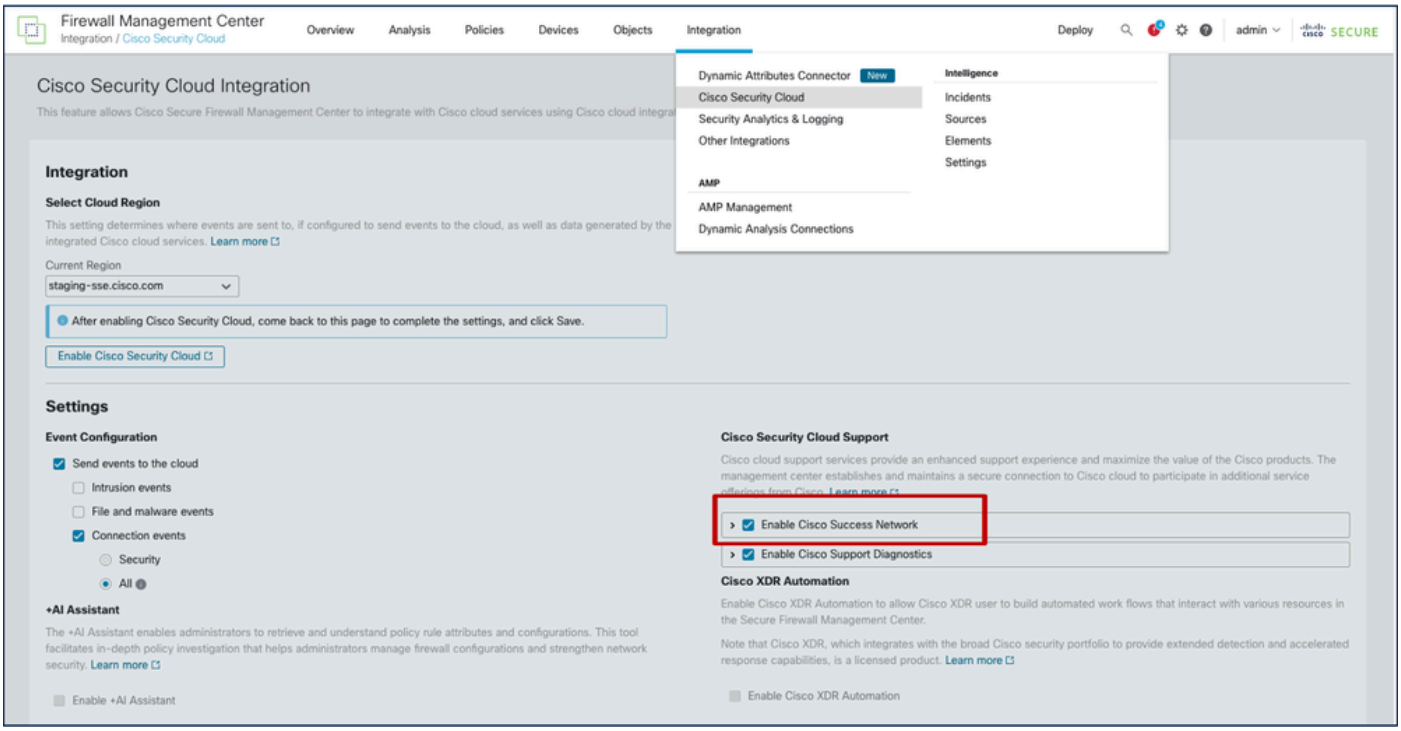
# 功能詳細資訊

## FMC UI

- Talos Threat Hunting Telemetry的「系統/配置/入侵策略首選項」頁面上的新功能標籤覈取方塊。
- 對於7.6.0上的新安裝以及升級到7.6.0的現有客戶，功能標籤預設設定為ON。
- 功能依賴於「啟用思科成功網路」。 必須同時啟用「啟用思科成功網路」和「Talos威脅搜尋遙測」選項。
- 如果兩者均未啟用，則_SSE_ThreatHunting.json consumer不會開啟，並且需要_SSE_ThreatHunting.json來處理事件並將其推送到SSE Connector。
- 功能標誌值向下同步到版本為7.6.0或更高的所有受管裝置。

## 工作方式






- 功能標誌儲存在FMC上的 — /etc/sf/threat_hunting.conf中。
- 此功能標誌值也儲存為/var/sf/tds/cloud-events.json中的「threat_hunting」，然後同步到/ngfw/var/tmp/tds-cloud-events.json上的受管裝置。
- 記錄以檢查標誌值是否未同步到FTD:
  - /var/log/sf/data_service.log。
  - FTD上的/ngfw/var/log/sf/data_service.log。

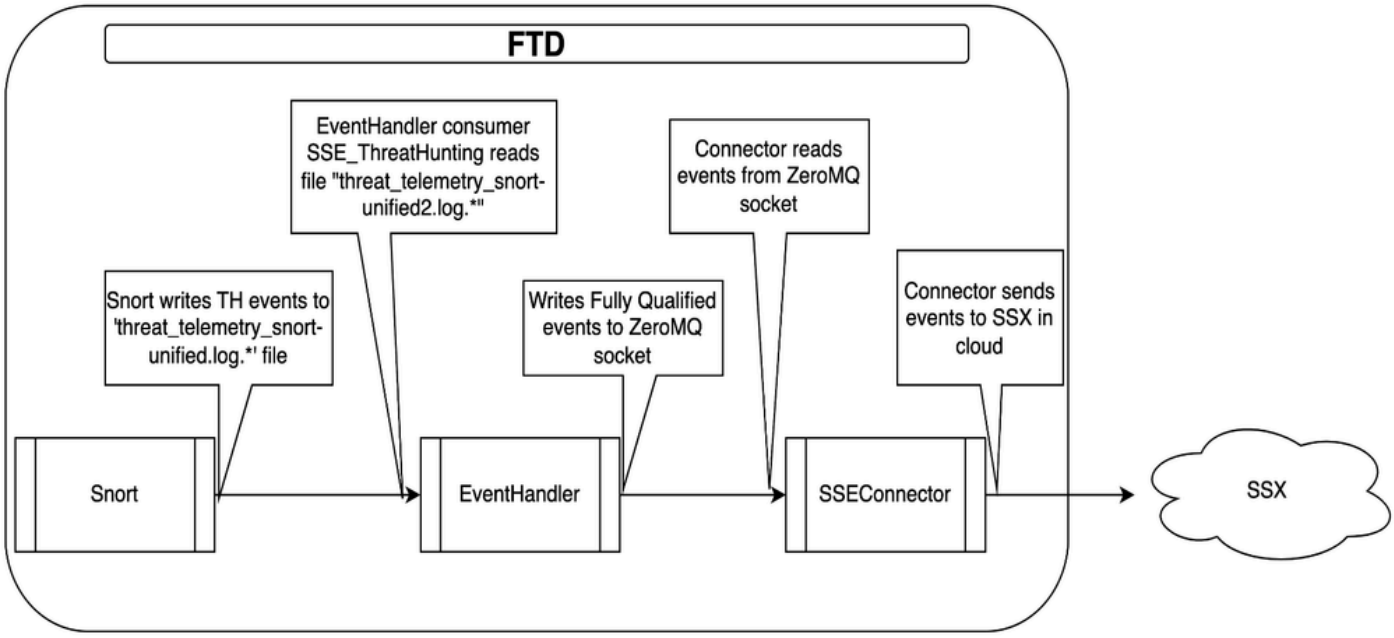
## Snort 3

- 處理威脅搜尋遙測(THT)規則的方式與處理常見IPS規則的方式相同。
- FTD u2unified logger將威脅搜尋遙測IPS事件僅寫入threat_telemetry_snort-unified.log.*。因此，FTD使用者看不到這些事件。新檔案與snort-unified.log位於同一目錄中。*
- 此外，威脅搜尋遙測事件包含用於規則評估的IPS緩衝區的轉儲。
- 作為IPS規則，威脅搜尋遙測規則是Snort端事件過濾的主題。但是，終端使用者無法為THT規則配置event_filter，因為它們未列在FMC中。

## 事件處理程式

- Snort在統一檔案字首threat_telemetry_snort-unified.log.*中生成入侵、資料包和外部事件。
- 裝置上的EventHandler處理這些事件，並通過SSX聯結器將它們傳送到雲。
- 這些事件的新EventHandler使用者：
  - /etc/sf/EventHandler/Consumers/SSE_ThreatHunting
  - 低優先順序執行緒 — 僅在有額外CPU可用時運行

### 工作方式




# 疑難排解

## EventHandler故障排除 — 裝置

- 在/ngfw/var/log/messages中查詢EventHandler日誌

```
Jan 11 21:26:01 firepower SF-IMS[39581]: [10055] EventHandler:EventHandler[INFO] Consumer SSE_ThreatHun
```

- 在/ngfw/var/log/EventHandlerStats檔案中查詢事件處理詳細資訊：

```
{"Time": "2024-01-11T21:26:01Z", "ConsumerStatus": "Start SSE_ThreatHunting", "TID": 10055}
{"Time": "2024-01-11T21:31:56Z", "Consumer": "SSE_ThreatHunting", "Events": 9, "PerSec": 0, "CPUSec": 0
{"Time": "2024-01-11T21:31:56Z", "ConsumerEvent": "SSE_ThreatHunting-IntrusionExtraData", "InTransforms
{"Time": "2024-01-11T21:31:56Z", "ConsumerEvent": "SSE_ThreatHunting-IntrusionPacket", "InTransforms":
{"Time": "2024-01-11T21:31:56Z", "ConsumerEvent": "SSE_ThreatHunting-IntrusionEvent", "InTransforms": 3
```

- 如果EventHandlerStats未顯示任何事件，則檢查Snort是否正在生成威脅查詢事件：

```
ls -l /ngfw/var/sf/detection_engines/*/instance-1 | grep unified
```

- 這些事件位於帶有「threat_telemetry_snort-unified.log」字首的檔案中
- 通過檢查以下輸出檢查檔案是否有所需事件：

```
u2dump output:u2dump/ngfw/var/sf/detection_engines/*/instance-1/threat_telemetry_snort-unified.log.1704
```

- 如果檔案不包含所需事件，請檢查：
  - 是否啟用威脅搜尋配置
  - Snort進程是否正在運行

## Snort組態疑難排解 — 裝置

- 檢查Snort配置是否啟用威脅搜尋遙測事件：

```
/ngfw/var/sf/detection_engines/
```

```
/snort3 --plugin-path /ngfw/var/sf/detection_engines/
```

```
/plugins:/ngfw/var/sf/lsp/active-so_rules-c /ngfw/var/sf/detection_engines/
```

```
/snort3.lua --dump-config-text 2>/dev/null | grep "sfunified2_logger.threat_hunting_telemetry_g
```

- 檢查是否存在並啟用威脅搜尋遙測規則：

```
/ngfw/var/sf/detection_engines/
```

```
/snort3 --plugin-path /ngfw/var/sf/detection_engines/
```

```
/plugins:/ngfw/var/sf/lsp/active-so_rules -c /ngfw/var/sf/detection_engines/
```

```
/snort3.lua -lua "process=nil" --dump-rule-state 2>/dev/null | grep "\"gid\": 6,"
```

- 威脅搜尋遙測規則包含在規則分析統計資訊中。因此，如果規則消耗了大量CPU時間，則在FMC頁面上的Rule Profiling statistics中可見這些規則。

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）。