7.6のTalos脅威ハンティングテレメトリ機能について

内容

はじめに
前提条件
- 要件
  - 最低限のソフトウェアおよびハードウェアプラットフォーム
- 使用するコンポーネント

機能の詳細
- FMCのUI
  - 仕組み
- Snort 3
- イベント処理
  - 仕組み

トラブルシューティング
- EventHandlerのトラブルシューティング – デバイス
- Snort設定のトラブルシューティング：デバイス

はじめに

このドキュメントでは、7.6のTalos脅威ハンティングテレメトリ機能について説明します。

前提条件

要件

最低限のソフトウェアおよびハードウェアプラットフォーム

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

- TalosがFirepowerデバイスにプッシュされる特別なクラスのルールを使用して、インテリジェンスと誤検出テストを収集する機能を提供します。
- これらのイベントはSSXコネクタ経由でクラウドに送信され、Talosによってのみ使用されます。
- グローバルポリシー設定の一部として脅威ハンティングルールを含む新機能のチェックボックス。
- 新しいログファイル(threat_telemetry_snort-unified.log.*)をinstance-*ディレクトリ内に作成し、侵入イベントのログを脅威ハンティングルールの一部として生成。

- 追加データの新しいレコードタイプとして脅威ハンティングルールのIPSバッファをダンプします。
- EventHandlerプロセスは、バンドルおよび圧縮された完全修飾形式でIPS/Packet/Extradataイベントをクラウドに送信するために新しいコンシューマを使用します。
- これらのイベントはFMC UIには表示されません

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

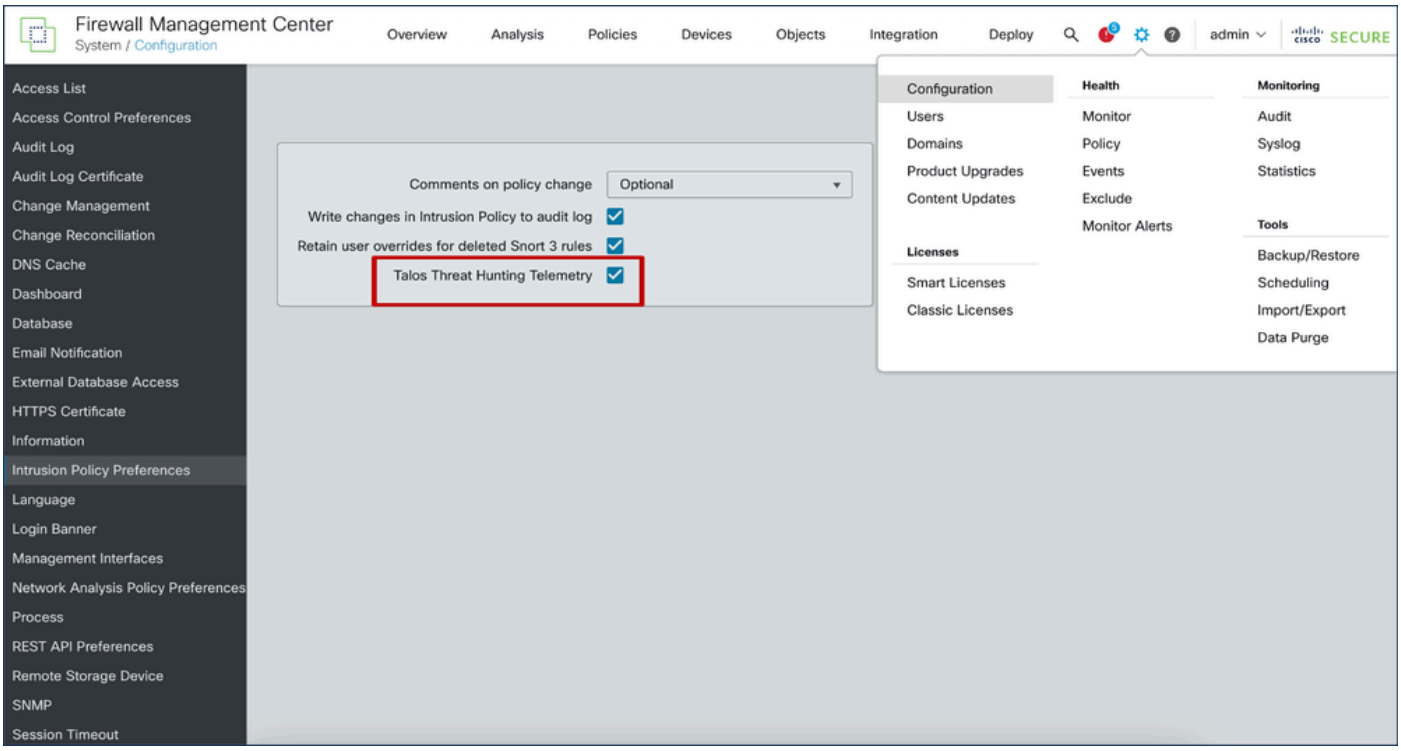
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

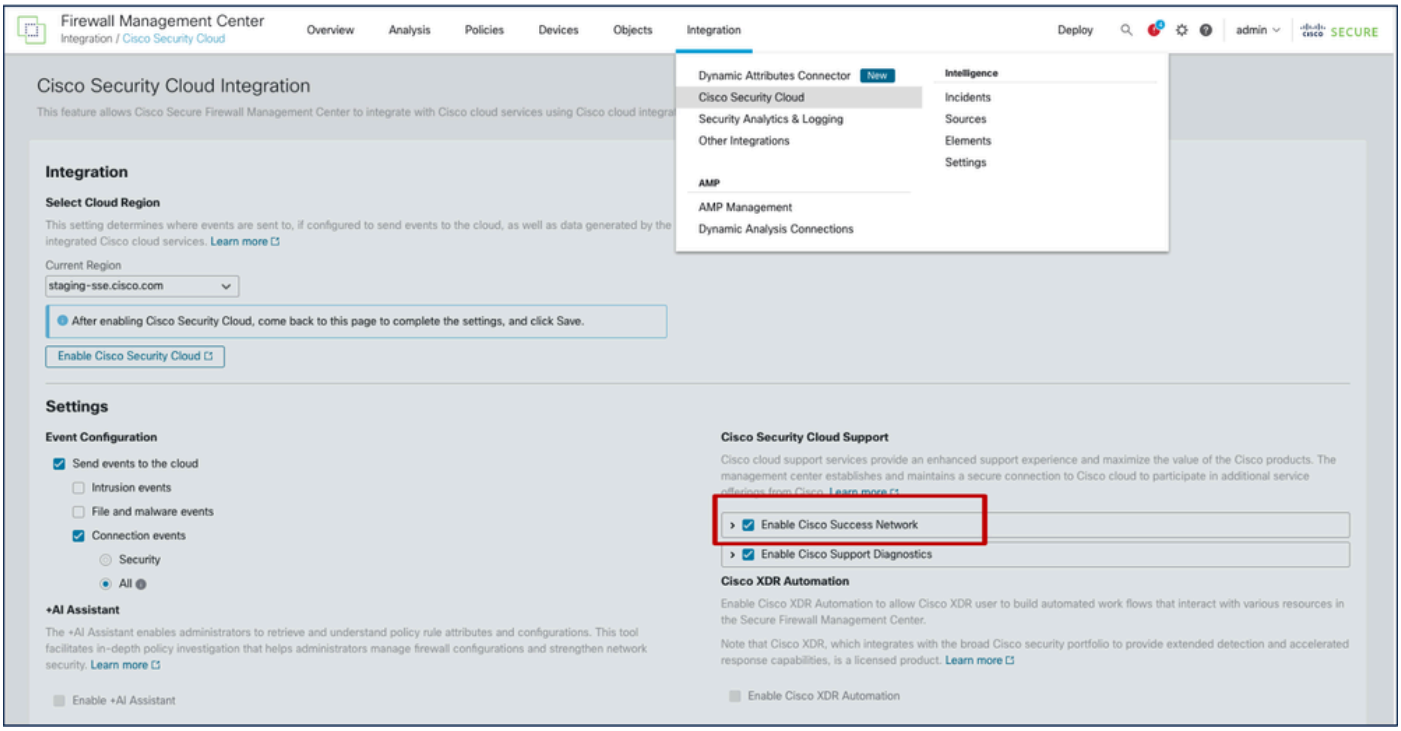
機能の詳細

FMCのUI

- Talos脅威ハンティングテレメトリのシステム/設定/侵入ポリシー設定ページの新機能フラグチェックボックス
- 機能フラグは、7.6.0での新規インストールと7.6.0へのアップグレードを行う既存のお客様の両方に対して、デフォルトでオンになっています。
- 機能は「Enable Cisco Success Network」に依存しています。 「Cisco Success Networkを有効にする」オプションと「Talos脅威ハンティングテレメトリ」オプションの両方を有効にする必要があります。
- 両方が有効になっていない場合、_SSE_ThreatHunting.jsonコンシューマは有効にならず、イベントを処理してSSEコネクタにプッシュするには_SSE_ThreatHunting.jsonが必要です。
- 機能フラグの値は、バージョン7.6.0以上のすべての管理対象デバイスに同期されます。

仕組み





- 機能フラグは、FMCの – /etc/sf/threat_hunting.confに保存されます。
- この機能フラグの値は、/var/sf/tds/cloud-events.jsonに「threat_hunting」として保存され、/ngfw/var/tmp/tds-cloud-events.jsonの管理対象デバイスに同期されます。
- フラグ値がFTDと同期しない場合に確認するログ：
  - FMCの/var/log/sf/data_service.log。
  - FTDの/ngfw/var/log/sf/data_service.log。

Snort 3

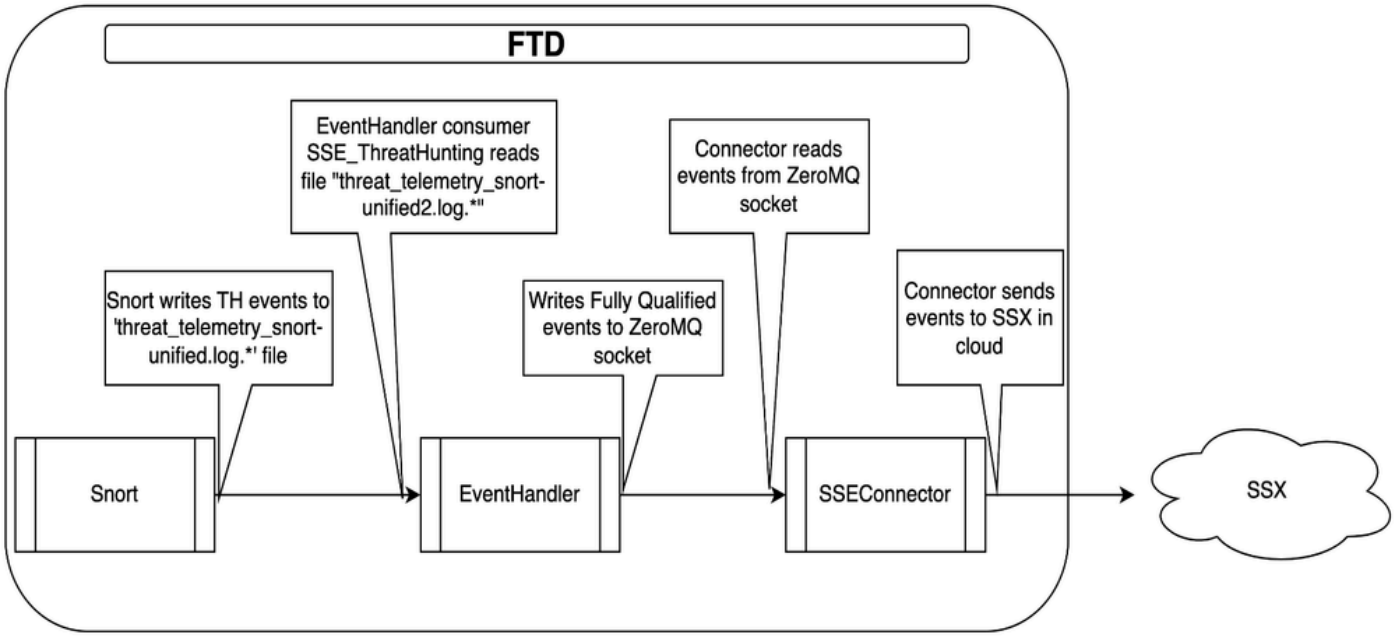
- 脅威ハンティングテレメトリ(THT)ルールは、一般的なIPSルールと同じように処理されま

す。
- FTD u2unified loggerは、threat_telemetry_snort-unified.log.*にのみ脅威ハンティングテレメトリIPSイベントを書き込みます。したがって、これらのイベントはFTDユーザには表示されません。新しいファイルはsnort-unified.logと同じディレクトリにあります。*
- さらに、脅威ハンティングテレメトリイベントには、ルール評価に使用されるIPSバッファのダンプが含まれます。
- IPSルールである脅威ハンティングテレメトリルールは、Snort側のイベントフィルタリングの対象となります。ただし、エンドユーザはFMCにリストされていないため、THTルールのevent_filterを設定できません。

イベント処理

- Snortは、侵入、パケット、および外部イベントをユニファイドファイルのプレフィクスthreat_telemetry_snort-unified.log.*に生成します。
- デバイスのEventHandlerがこれらのイベントを処理し、SSXコネクタ経由でクラウドに送信します。
- これらのイベントの新しいEventHandlerコンシューマー：
  - /etc/sf/EventHandler/Consumers/SSE_ThreatHunting
  - 低優先順位スレッド – 追加のCPUが利用可能な場合にのみ実行されます

仕組み



トラブルシューティング

EventHandlerのトラブルシューティング – デバイス

- /ngfw/var/log/messagesでEventHandlerログを検索します

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

- イベント処理の詳細については、/ngfw/var/log/EventHandlerStatsファイルを参照してください。

```
{"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
```

- EventHandlerStatsにイベントが表示されない場合は、Snortによって脅威ハンティングイベントが生成されているかどうかを確認します。

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

- イベントは、プレフィックス「threat_telemetry_snort-unified.log」が付いたファイルに含まれています
- 次の出力を調べて、目的のイベントのファイルを確認します。

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

- ファイルに目的のイベントが含まれていない場合は、次の点を確認します。
  - 脅威ハンティングの設定が有効かどうか
  - Snortprocessが実行されているかどうか

Snort設定のトラブルシューティング：デバイス

- Snortの設定で脅威ハンティングテレメトリイベントが有効になっているかどうかを確認します。

```
/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_
```

- 脅威ハンティングテレメトリルールが存在し、有効になっているかどうかを確認します。

```
/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,"
```

- 脅威ハンティングテレメトリルールは、ルールプロファイリング統計情報に含まれます。そのため、ルールが多くのCPU時間を消費する場合、FMCページのルールプロファイリング統計情報に表示されます。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。