# Comprendre la fonction de télémétrie de recherche des menaces de Talos dans 7.6

## Table des matières



## Introduction

Ce document décrit la fonctionnalité de télémétrie de recherche de menaces Talos de la version 7.6.

## Conditions préalables

### Exigences

#### Plates-formes logicielles et matérielles minimales

| 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 |

- Permet à Talos de collecter des informations et des faux positifs via une classe spéciale de règles appliquées aux périphériques Firepower.
- Ces événements sont envoyés au cloud via le connecteur SSX et ils sont consommés uniquement par Talos.
- Une nouvelle case à cocher de fonctionnalité qui inclut les règles de recherche de menace dans la configuration de la stratégie globale.
- Un nouveau fichier journal (threat_telemetry_snort-unified.log.*) dans le répertoire instance-*

pour consigner les événements d'intrusion générés dans le cadre des règles de recherche de menaces.
- Vider les mémoires tampon IPS pour les règles de recherche de menace en tant que nouveau type d'enregistrement dans les données supplémentaires.
- Le processus EventHandler utilise un nouveau consommateur pour envoyer des événements IPS/Packet/Extradata au cloud dans un format complet, groupé et compressé.
- Ces événements ne sont pas affichés dans l'interface utilisateur FMC

### Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

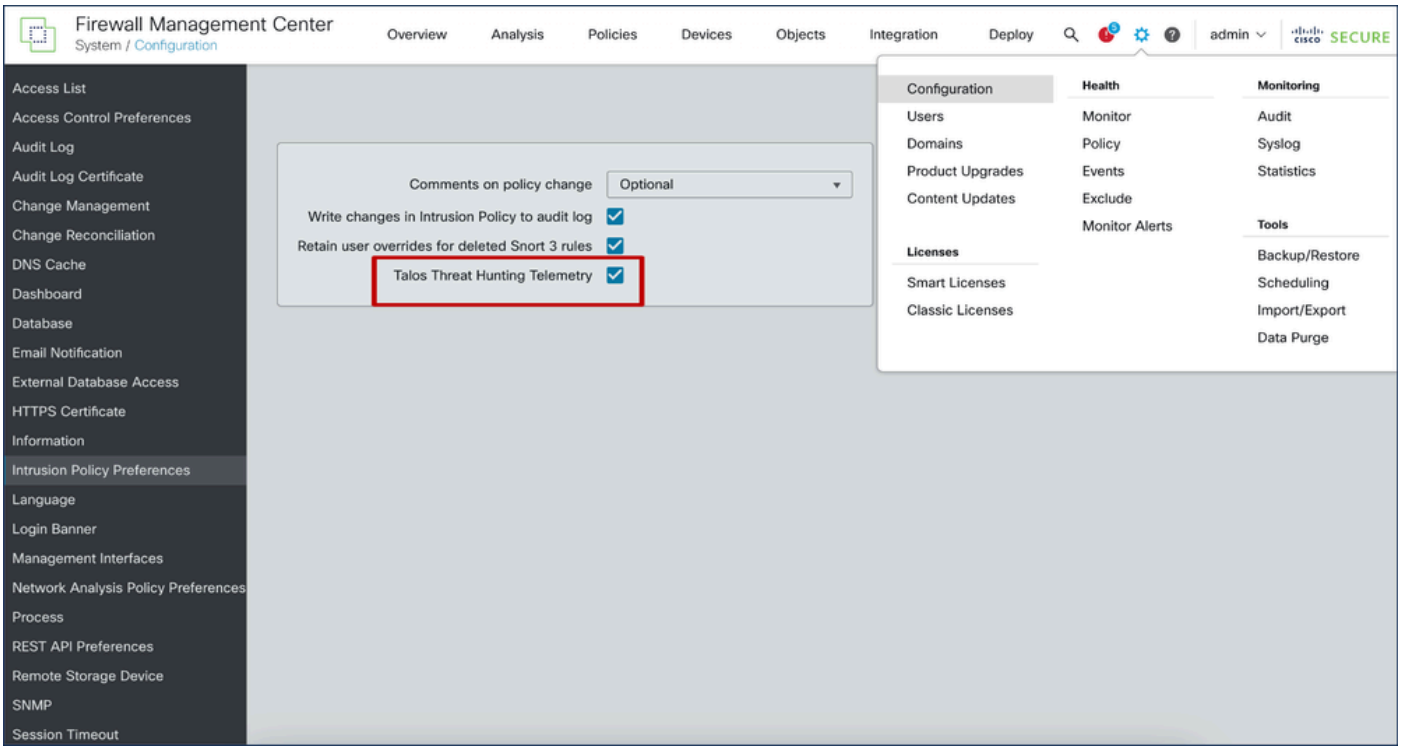
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

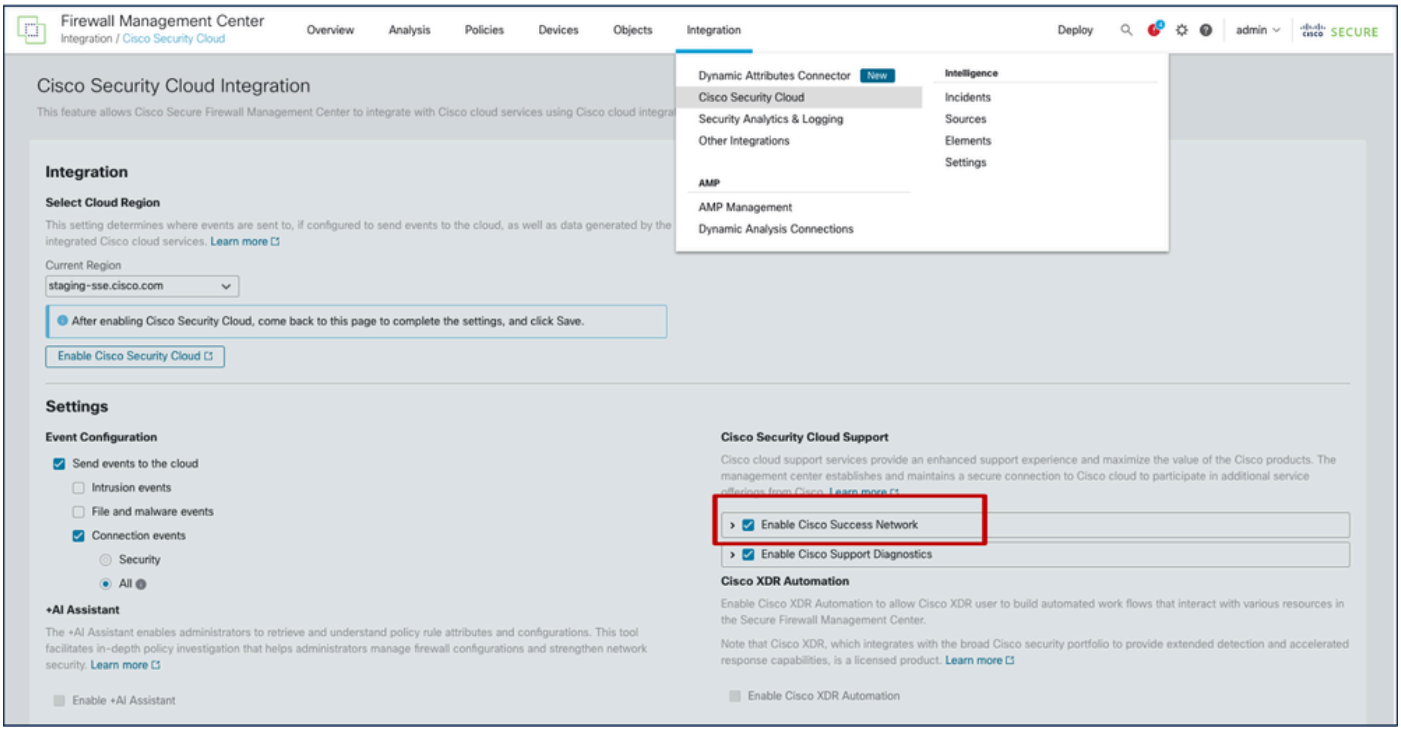
## Détails des fonctionnalités

### Interface utilisateur FMC

- Case à cocher Nouvel indicateur de fonctionnalité de la page Système / Configuration / Préférences de stratégie d'intrusion pour la télémétrie de recherche de menaces Talos.
- L'indicateur de fonctionnalité est ON par défaut, à la fois pour les nouvelles installations sur 7.6.0 et pour les clients existants effectuant une mise à niveau vers 7.6.0.
- La fonction dépend de « Enable Cisco Success Network ».  Les options « Enable Cisco Success Network » et « Talos Threat Hunting Telemetry » doivent toutes deux être activées.
- Si les deux ne sont pas activés, le consommateur _SSE_ThreatHunting.json ne s'active pas et _SSE_ThreatHunting.json est nécessaire pour traiter et transmettre les événements au connecteur SSE.
- La valeur de l'indicateur de fonctionnalité est synchronisée avec tous les périphériques gérés avec les versions 7.6.0 ou ultérieures.

Comment ça fonctionne




- L'indicateur de fonction est stocké dans - /etc/sf/threat_hunting.conf sur FMC.
- Cette valeur d'indicateur de fonctionnalité est également enregistrée en tant que « threat_hunter » dans /var/sf/tds/cloud-events.json, qui se synchronise ensuite sur les périphériques gérés à l'adresse /ngfw/var/tmp/tds-cloud-events.json.
- Journaux pour vérifier si la valeur de l'indicateur n'est pas synchronisée avec les FTD :
  - /var/log/sf/data_service.log sur FMC.
  - /ngfw/var/log/sf/data_service.log sur FTD.

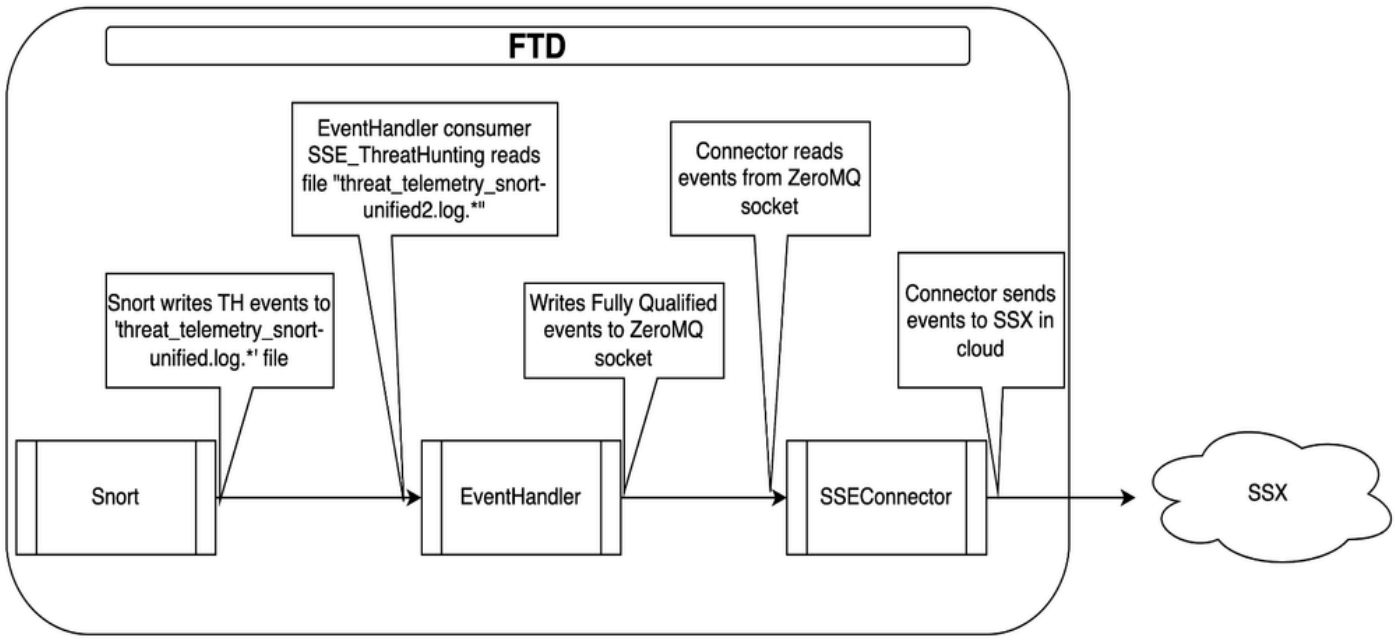
## Snort 3

- Les règles THT (Threat Hunting Telemetry) sont traitées de la même manière que les règles IPS courantes.
- FTD u2unified logger écrit les événements IPS de télémétrie de recherche de menace uniquement dans threat_telemetry_snort-unified.log.*. Par conséquent, ces événements ne sont pas visibles pour l'utilisateur FTD. Le nouveau fichier se trouve dans le même répertoire que snort-unified.log.*
- En outre, les événements de télémétrie de recherche de menaces contiennent un vidage des mémoires tampons IPS utilisées pour l'évaluation des règles.
- Étant une règle IPS, la règle de télémétrie de recherche de menaces est un sujet pour le filtrage des événements côté Snort. Cependant, l'utilisateur final ne peut pas configurer event_filter pour les règles THT, car elles ne sont pas répertoriées dans FMC.

### Gestionnaire d’événements

- Snort génère des événements d'intrusion, de paquet et d'extradata dans le préfixe de fichier unifié threat_telemetry_snort-unified.log.*.
- EventHandler sur le périphérique traite ces événements et les envoie au cloud via le connecteur SSX.
- Nouveau consommateur EventHandler pour ces événements :
  - /etc/sf/EventHandler/Consumers/SSE_ThreatHunting
  - Thread de faible priorité : s'exécute uniquement lorsque du processeur supplémentaire est disponible

Comment ça fonctionne




## Dépannage

### Dépannage de EventHandler - Périphérique

- Rechercher dans /ngfw/var/log/messages les journaux EventHandler

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

- Recherchez dans le fichier /ngfw/var/log/EventHandlerStats les détails du traitement des événements :

```
{"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
```

- Si EventHandlerStats n'affiche aucun événement, vérifiez si Snort génère des événements de recherche de menace :

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

- Les événements se trouvent dans les fichiers avec le préfixe « threat_telemetry_snort-unified.log »
- Recherchez les événements souhaités dans les fichiers en inspectant cette sortie :

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

- Si les fichiers ne contiennent pas les événements souhaités, vérifiez les points suivants :
  - Indique si la configuration de recherche de menaces est activée
  - Indique si Snortprocess est en cours d'exécution

## Dépannage de la configuration Snort - Périphérique

- Vérifiez si la configuration Snort active les événements de télémétrie de recherche de menaces :

```
/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
```

- Vérifiez si les règles de télémétrie de recherche de menaces sont présentes et activées :

```
/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,"
```

- Les règles de télémétrie de recherche de menaces sont incluses dans les statistiques de

profilage de règles. Ainsi, si les règles consomment beaucoup de temps processeur, elles sont visibles dans les statistiques de profilage de règle sur la page FMC.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.