Funktionen der Talos Threat Hunting-Telemetrie in 7.6

Inhalt

Einleitung

In diesem Dokument wird die Funktion Talos Threat Hunting Telemetry in Abschnitt 7.6 beschrieben.

Voraussetzungen

Anforderungen

Software- und Hardware-Mindestanforderungen

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

- Bietet Talos die Möglichkeit, Informationen zu sammeln und Fehlalarme über spezielle Regelklassen zu testen, die auf die FirePOWER-Geräte übertragen werden.
- Diese Ereignisse werden über SSX Connector an die Cloud gesendet und nur von Talos verbraucht.
- Ein neues Feature-Kontrollkästchen, das die Regeln zur Nachverfolgung von Bedrohungen als Teil der globalen Richtlinienkonfiguration enthält.
- Eine neue Protokolldatei (Threat_telemetry_snort-unified.log.*) im instanz-* Verzeichnis, um

die Angriffsereignisse zu protokollieren, die als Teil der Regeln für das Sammeln von Bedrohungen generiert werden.
- IPS-Puffer für die Regeln zur Nachverfolgung von Bedrohungen als neuen Datensatztyp in zusätzlichen Daten speichern.
- Der EventHandler-Prozess verwendet einen neuen Consumer, um IPS-/Packet-/Extradata-Ereignisse in vollständig qualifiziertem, gebündeltem und komprimiertem Format an die Cloud zu senden.
- Diese Ereignisse werden nicht in der FMC-Benutzeroberfläche angezeigt.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

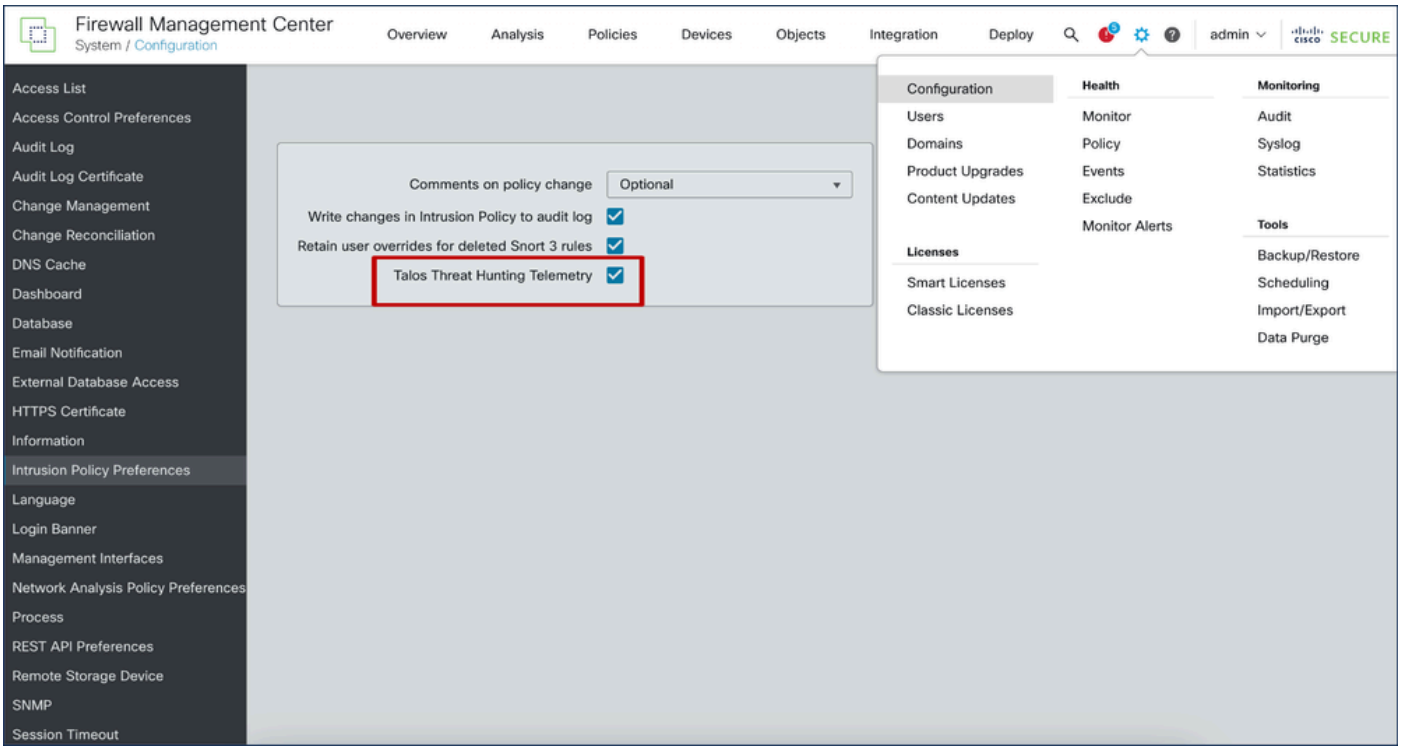
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

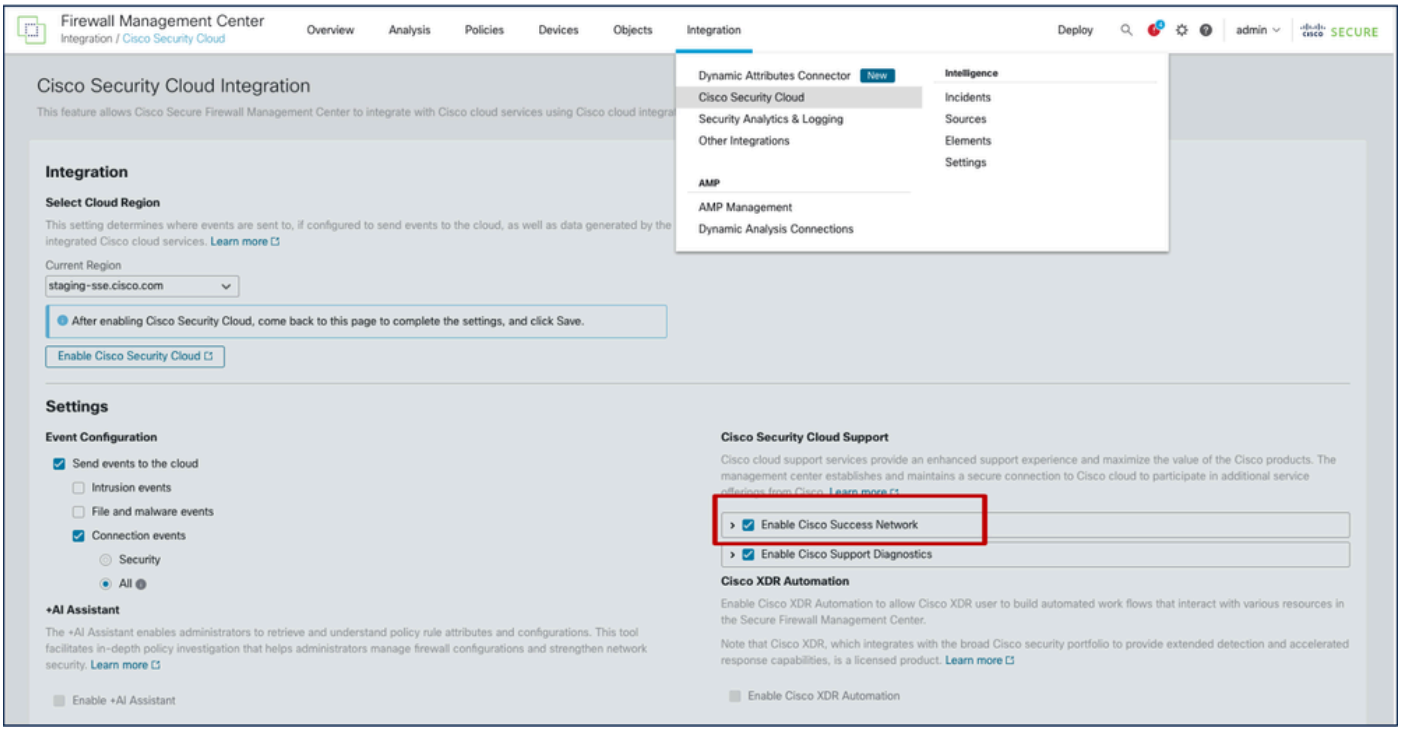
Funktionsdetails

FMC-Benutzeroberfläche

- Neues Feature-Kontrollkästchen auf der Seite "System/Konfiguration/Intrusion Policy Preference" (Voreinstellungen für System/Konfiguration/Angriffsrichtlinie) für Talos Threat Hunting Telemetry.
- Das Feature-Flag ist standardmäßig aktiviert, sowohl für neue Installationen auf 7.6.0 als auch für bestehende Kunden, die ein Upgrade auf 7.6.0 durchführen.
- Die Funktion ist abhängig von der Aktivierung des Cisco Success Network. Sowohl die Optionen "Cisco Success Network aktivieren" als auch "Talos Threat Hunting Telemetry" müssen aktiviert sein.
- Wenn beide nicht aktiviert sind, wird _SSE_ThreatHunting.json consumer nicht aktiviert, und _SSE_ThreatHunting.json ist erforderlich, um die Ereignisse zu verarbeiten und an SSE Connector weiterzuleiten.
- Der Feature-Flag-Wert wird auf alle verwalteten Geräte mit Version 7.6.0 oder höher synchronisiert.

So funktioniert es





- Das Feature-Flag wird in - /etc/sf/threat_hunting.conf auf FMC gespeichert.
- Dieser Wert für das Feature-Flag wird auch als "Threat_hunting" in /var/sf/tds/cloud-events.json gespeichert, das dann auf verwaltete Geräte unter /ngfw/var/tmp/tds-cloud-events.json heruntersynchronisiert wird.
- Protokolle zur Überprüfung, ob der Flagwert nicht mit FTDs synchronisiert wird:
  - /var/log/sf/data_service.log auf FMC.
  - /ngfw/var/log/sf/data_service.log auf FTD.

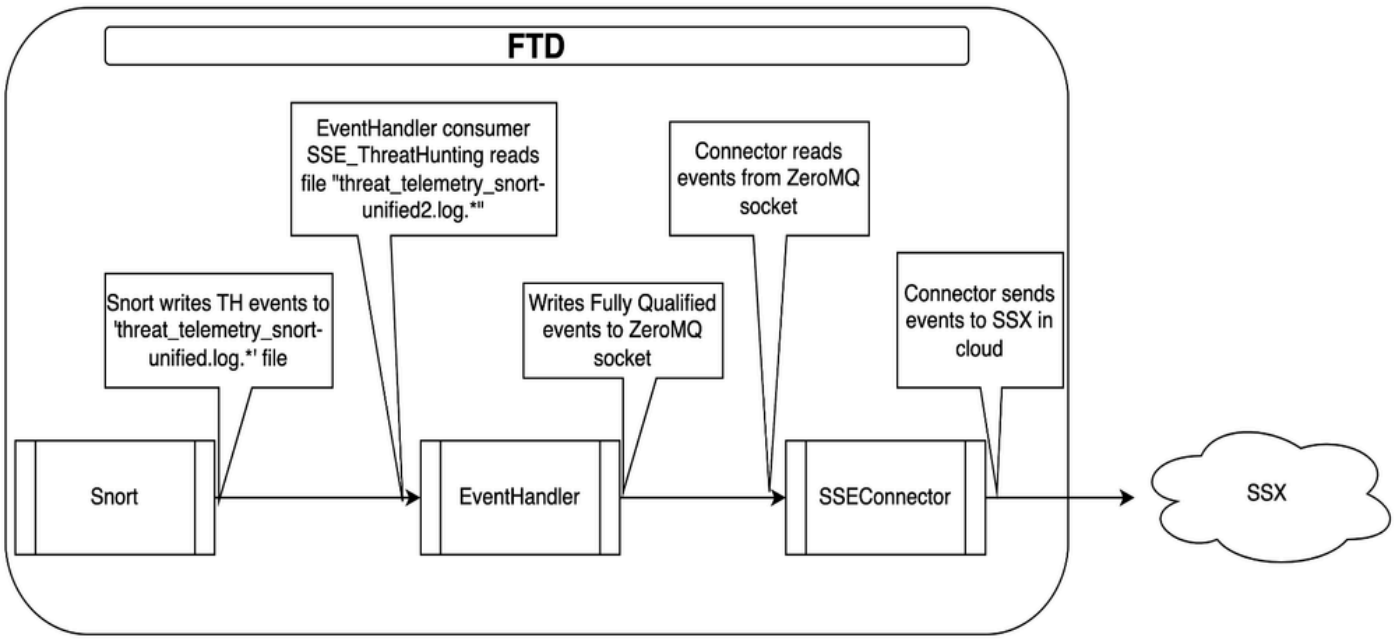
Snort 3

- THT-Regeln (Threat Hunting Telemetry) werden auf die gleiche Weise verarbeitet wie allgemeine IPS-Regeln.
- FTD u2unified logger schreibt Bedrohungs-Jagd-Telemetrie-IPS-Ereignisse nur in Threat_telemetry_snort-unified.log.*. Daher sind diese Ereignisse für FTD-Benutzer nicht sichtbar. Die neue Datei befindet sich im gleichen Verzeichnis wie snort-unified.log.*
- Zusätzlich enthalten Threat Hunting-Telemetrieereignisse einen Dump von IPS-Puffern, die für die Regelauswertung verwendet werden.
- Da es sich um eine IPS-Regel handelt, ist die Telemetrieregel zur Nachverfolgung von Bedrohungen ein Thema für die Ereignisfilterung auf Snort-Seite. Der Endbenutzer kann event_filter jedoch nicht für THT-Regeln konfigurieren, da diese nicht im FMC aufgeführt sind.

Ereignishandler

- Snort generiert Intrusion-, Packet- und Extradataereignisse im Unified-Datei-Präfix threat_telemetry_snort-unified.log.*.
- EventHandler auf dem Gerät verarbeitet diese Ereignisse und sendet sie über SSX Connector an die Cloud.
- Neuer EventHandler-Consumer für diese Ereignisse:
  - /etc/sf/EventHandler/Consumers/SSE_ThreatHunting
  - Thread mit niedriger Priorität - Wird nur ausgeführt, wenn zusätzliche CPU verfügbar ist

So funktioniert es



Fehlerbehebung

EventHandler-Fehlerbehebung - Gerät

- Suchen Sie in /ngfw/var/log/messages nach EventHandler-Protokollen.

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

- Weitere Informationen zur Ereignisverarbeitung finden Sie in der Datei /ngfw/var/log/EventHandlerStats:

```
{"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
```

- Wenn EventHandlerStats keine Ereignisse anzeigt, prüfen Sie, ob Snort Ereignisse zur Bedrohungssuche generiert:

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

- Die Ereignisse befinden sich in den Dateien mit dem Präfix "threat_telemetry_snort-unified.log"
- Überprüfen Sie die Dateien auf die gewünschten Ereignisse, indem Sie diese Ausgabe überprüfen:

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

- Wenn die Dateien nicht die gewünschten Ereignisse enthalten, überprüfen Sie Folgendes:
  - Legt fest, ob die Konfiguration für die Nachverfolgung von Bedrohungen aktiviert ist.
  - Ob Snortprocess läuft oder nicht

Fehlerbehebung bei Snort-Konfiguration - Gerät

- Überprüfen Sie, ob die Snort-Konfiguration Telemetrieereignisse für die Nachverfolgung von Bedrohungen aktiviert:

```
/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
```

- Überprüfen Sie, ob Telemetrieregeln für die Nachverfolgung von Bedrohungen vorhanden und aktiviert sind:

```
/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,"
```

- Telemetrieregeln für die Nachverfolgung von Bedrohungen sind in den Statistiken zur Regelprofilierung enthalten. Wenn die Regeln also viel CPU-Zeit beanspruchen, werden sie in den Statistiken zur Regelprofilierung auf der Seite FMC angezeigt.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.