Kenmerken van Talos Threat Hunting-telemetrie in 7.6

Inhoud

Inleiding

Voorwaarden

- Vereisten
  - Minimale software- en hardwareplatforms
- Gebruikte componenten

Functiedetails

- FMC UI
  - Hoe het werkt
- Sorteren 3
- Event Handler
  - Hoe het werkt

Probleemoplossing

- Problemen oplossen bij EventHandler - Apparaat
- Probleemoplossing voor snurfconfiguratie - Apparaat

Inleiding

In dit document wordt de functie Talos Threat Hunting Telemetry in 7.6 beschreven.

Voorwaarden

Vereisten

Minimale software- en hardwareplatforms

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

- Biedt mogelijkheden voor Talos om intelligentie te verzamelen en vals-positieve testen via speciale klasse van regels die naar de vuurkracht apparaten worden geduwd.
- Deze gebeurtenissen worden naar de cloud gestuurd via SSX-connector, en ze worden alleen door Talos geconsumeerd.
- Een nieuwe optie checkbox die de bedreigingsjachtregels omvat als deel van de wereldwijde beleidsconfiguratie.
- Een nieuw logbestand (threat_telemetry_snort-unified.log.*) in de directory instantie-* om de inbraakgebeurtenissen te registreren die worden gegenereerd als deel van de regels voor

bedreigingsjacht.
- Dump IPS-buffers voor de bedreigingsjachtregels als een nieuw recordtype in extra gegevens.
- Het EventHandler-proces gebruikt een nieuwe consument om IPS/Packet/Extradata-gebeurtenissen naar de cloud te sturen in volledig gekwalificeerd formaat, gebundeld en gecomprimeerd.
- Deze gebeurtenissen worden niet weergegeven in de FMC UI

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

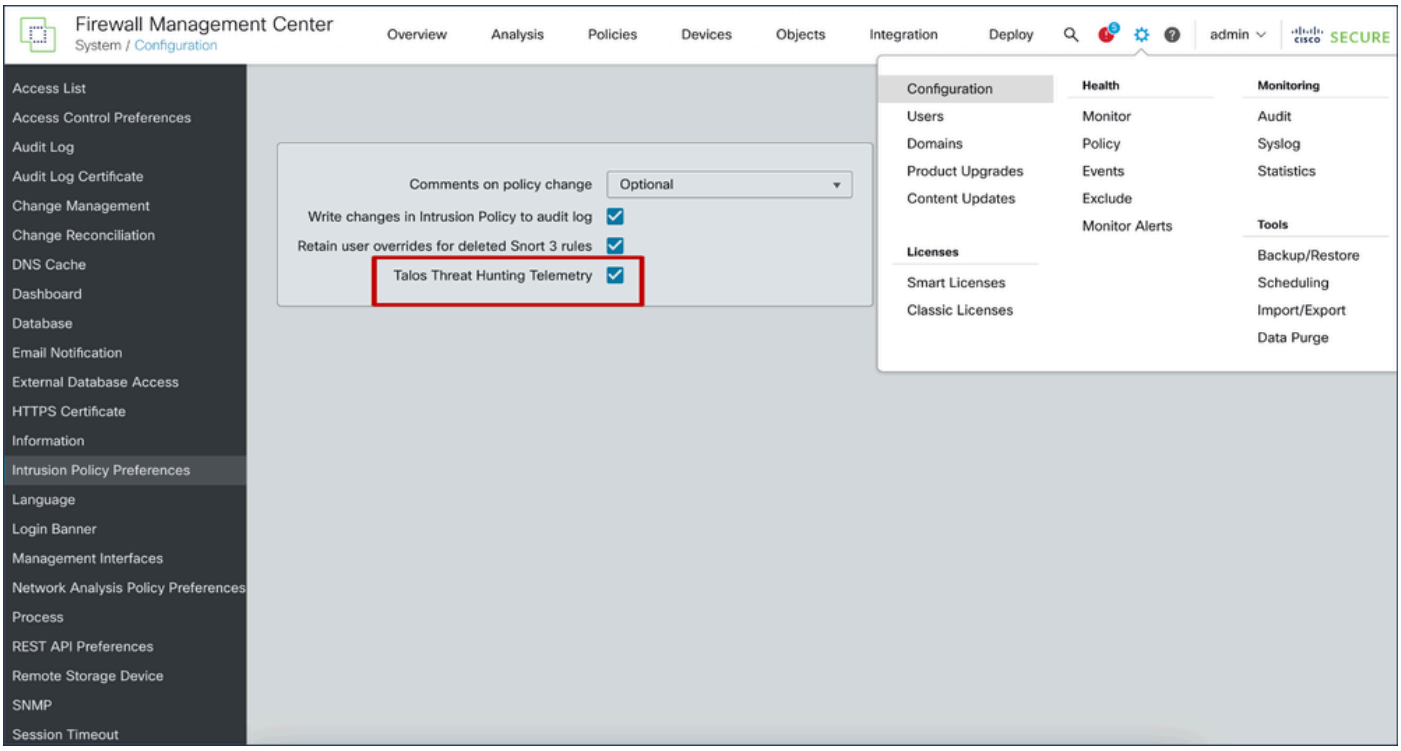
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

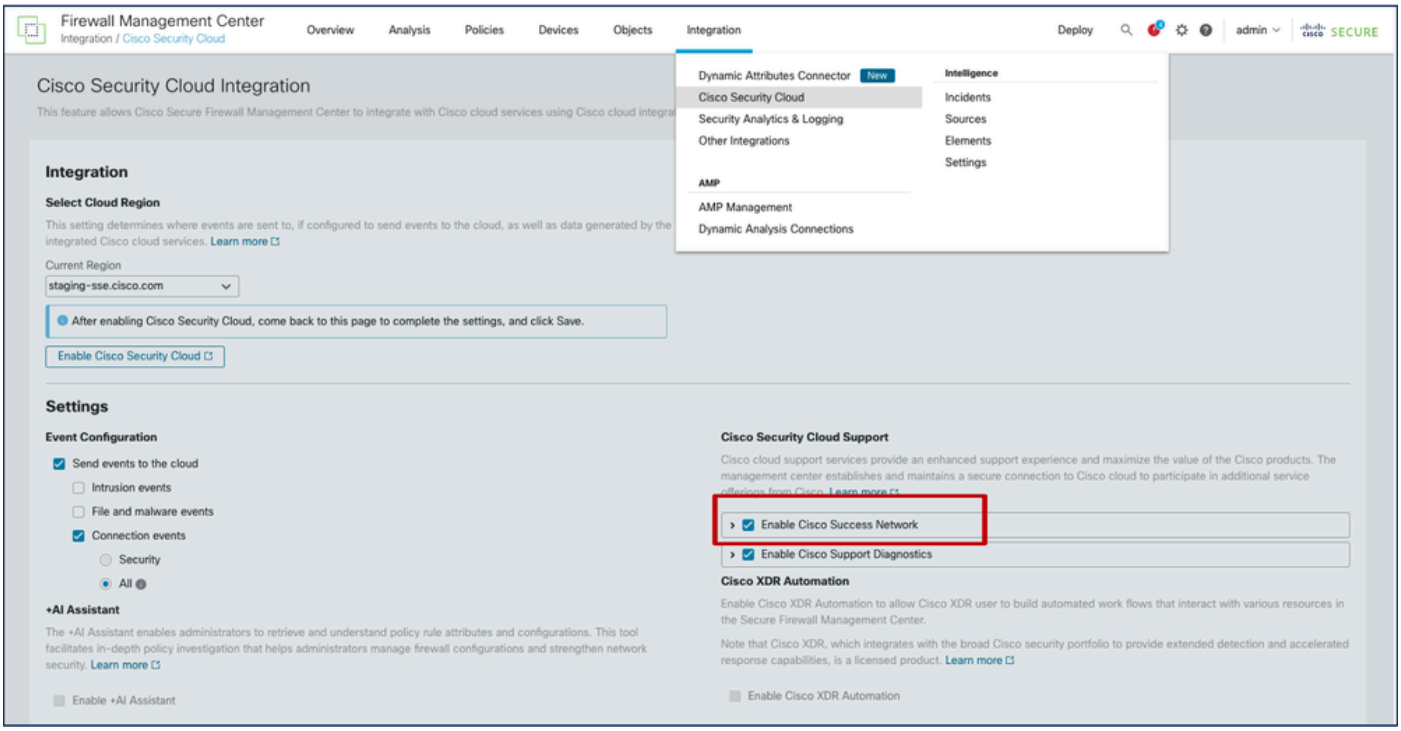
Functiedetails

FMC UI

- Selectievakje voor nieuwe functievlag op de voorkeurpagina voor systeem/configuratie/inbraakbeleid voor Talos Threat Hunting Telemetry.
- De functievlag is standaard ingeschakeld, zowel voor nieuwe installaties op 7.6.0 als voor bestaande klanten die upgraden naar 7.6.0.
- De functie is afhankelijk van "Cisco Success Network inschakelen". De opties "Cisco Success Network inschakelen" en "Talos Threat Hunting Telemetry" moeten zijn ingeschakeld.
- Als beide niet zijn ingeschakeld, wordt de consument van _SSE_ThreatHunting.json niet ingeschakeld en is _SSE_ThreatHunting.json nodig om de gebeurtenissen te verwerken en naar SSE Connector te duwen.
- De waarde van de eigenschapvlag synchroniseert neer aan alle beheerde apparaten met versies 7.6.0 of groter.

Hoe het werkt





- De vlag van de functie wordt opgeslagen in - /etc/sf/threat_hunting.conf op FMC.
- Deze waarde van de eigenschapvlag wordt ook opgeslagen als "threat_hunting" in /var/sf/tds/cloud-events.json, die dan aan beheerde apparaten in /ngfw/var/tmp/tds-cloud-events.json synchroniseert.
- Logbestanden om te controleren of de vlagwaarde niet synchroniseert naar FTD's:
  - /var/log/sf/data_service.log op FMC.
  - /ngfw/var/log/sf/data_service.log op FTD.

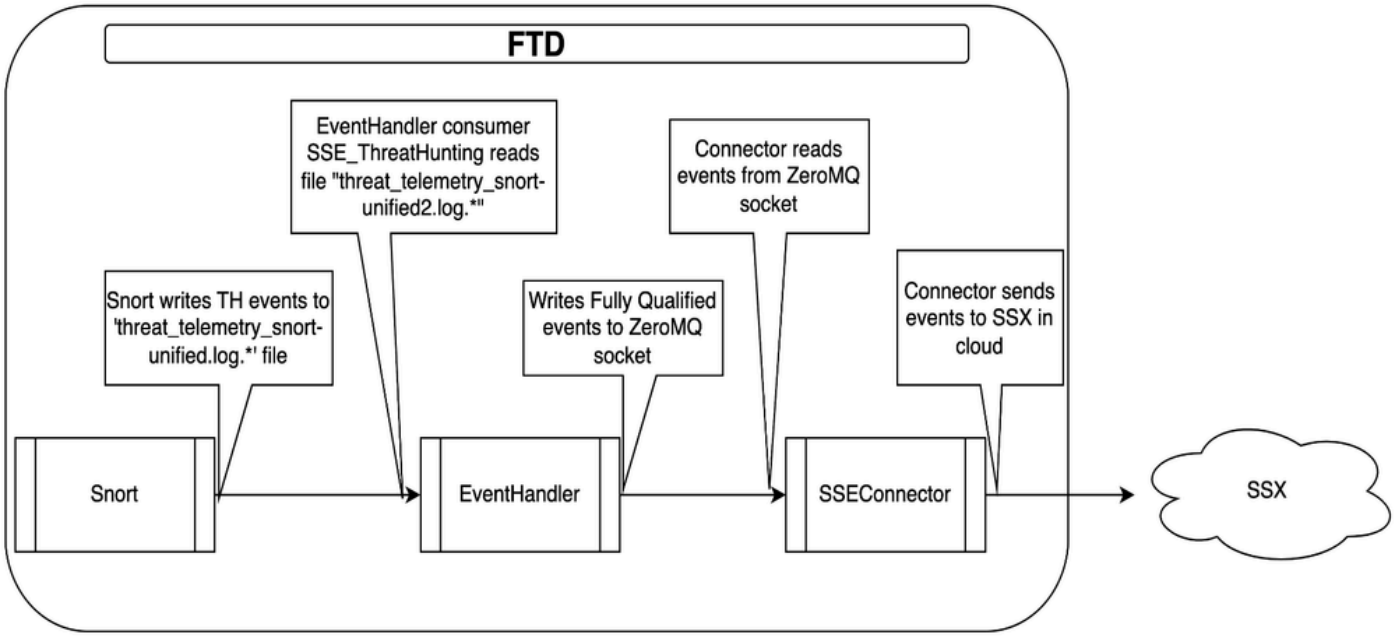
Sorteren 3

- Threat Hunting Telemetry (THT)-regels worden op dezelfde manier verwerkt als gemeenschappelijke IPS-regels.
- FTD u2unified logger schrijft bedreigingsjacht telemetrie IPS gebeurtenissen alleen naar threat_telemetry_snort-unified.log.*. Deze gebeurtenissen zijn dus niet zichtbaar voor FTD-gebruikers. Het nieuwe bestand bevindt zich in dezelfde map als snort-unified.log.*
- Bovendien bevatten de gebeurtenissen van de bedreigingsjacht telemetrie een stortplaats van IPS buffers die voor regelevaluatie worden gebruikt.
- Aangezien het een IPS-regel is, is de bedreigingsjacht telemetrieregel een onderwerp voor gebeurtenis het filtreren aan de kant van de Snort. De eindgebruiker kan event_filter echter niet voor THT regels configureren, omdat deze niet in FMC worden vermeld.

Event Handler

- Snort genereert inbraakproces, pakketgebeurtenissen en extradatagebeurtenissen in het Unified file prefix threat_telemetry_snort-unified.log.*.
- EventHandler op apparaat verwerkt deze gebeurtenissen en stuurt ze via SSX-connector naar de cloud.
- Nieuwe EventHandler consument voor deze evenementen:
  - /etc/sf/EventHandler/Consumers/SSE_ThreatHunting
  - thread met lage prioriteit - Wordt alleen uitgevoerd als er een extra CPU beschikbaar is

Hoe het werkt



Probleemoplossing

Problemen oplossen bij EventHandler - Apparaat

- Zoeken in /ngfw/var/log/berichten voor EventHandler logboeken

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

- Bekijk het bestand /ngfw/var/log/EventHandlerStats voor meer informatie over de gebeurtenisverwerking:

```
{"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
```

- Als EventHandlerStats geen gebeurtenissen toont, controleer dan of Snort bedreigingsjachtgebeurtenissen genereert:

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

- De gebeurtenissen bevinden zich in de bestanden met de prefix "threat_telemetry_snort-unified.log"
- Controleer de bestanden op de gewenste gebeurtenissen door deze uitvoer te inspecteren:

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

- Als de bestanden niet de gewenste gebeurtenissen bevatten, controleert u:
  - Of de configuratie van de Threat Hunting al dan niet is ingeschakeld
  - Of Snortprocess nu actief is of niet

Probleemoplossing voor snurfconfiguratie - Apparaat

- Controleer of de configuratie van de snort bedreigingsjacht met telemetrie mogelijk maakt:

```
/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
```

- Controleer of er telemetrieregels voor bedreigingsjacht aanwezig zijn en ingeschakeld zijn:

```
/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,"
```

- De regels van de bedreigingsjacht telemetrie zijn inbegrepen in de statistieken van het Regel Profileren. Dus als de regels veel CPU-tijd verbruiken, zijn ze zichtbaar in Regel Profiling statistieken op FMC pagina.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.