Compreenda o recurso Threat Hunting Telemetry da Talos na versão 7.6

Contents

Introdução

Este documento descreve o recurso Threat Hunting Telemetry do Talos na versão 7.6.

Pré-requisitos

Requisitos

Plataformas mínimas de software e hardware

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

- Fornece a capacidade para que o Talos colete informações e testes falsos positivos por meio de uma classe especial de regras enviadas para os dispositivos Firepower.
- Esses eventos são enviados para a nuvem através do conector SSX e são consumidos apenas pelo Talos.
- Uma caixa de seleção de novo recurso que inclui as regras de busca de ameaças como parte da configuração de política global.
- Um novo arquivo de registro (threat_telemetry_snort-unified.log.*) dentro do diretório instance-* para registrar os eventos de intrusão gerados como parte das regras de busca de

ameaças.
- Descartar buffers IPS para as regras de busca de ameaças como um novo tipo de registro em dados extras.
- O processo EventHandler usa um novo consumidor para enviar eventos de IPS/Pacote/Extradata para a nuvem em formato totalmente qualificado, agrupado e compactado.
- Esses eventos não são exibidos na interface do usuário do FMC

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

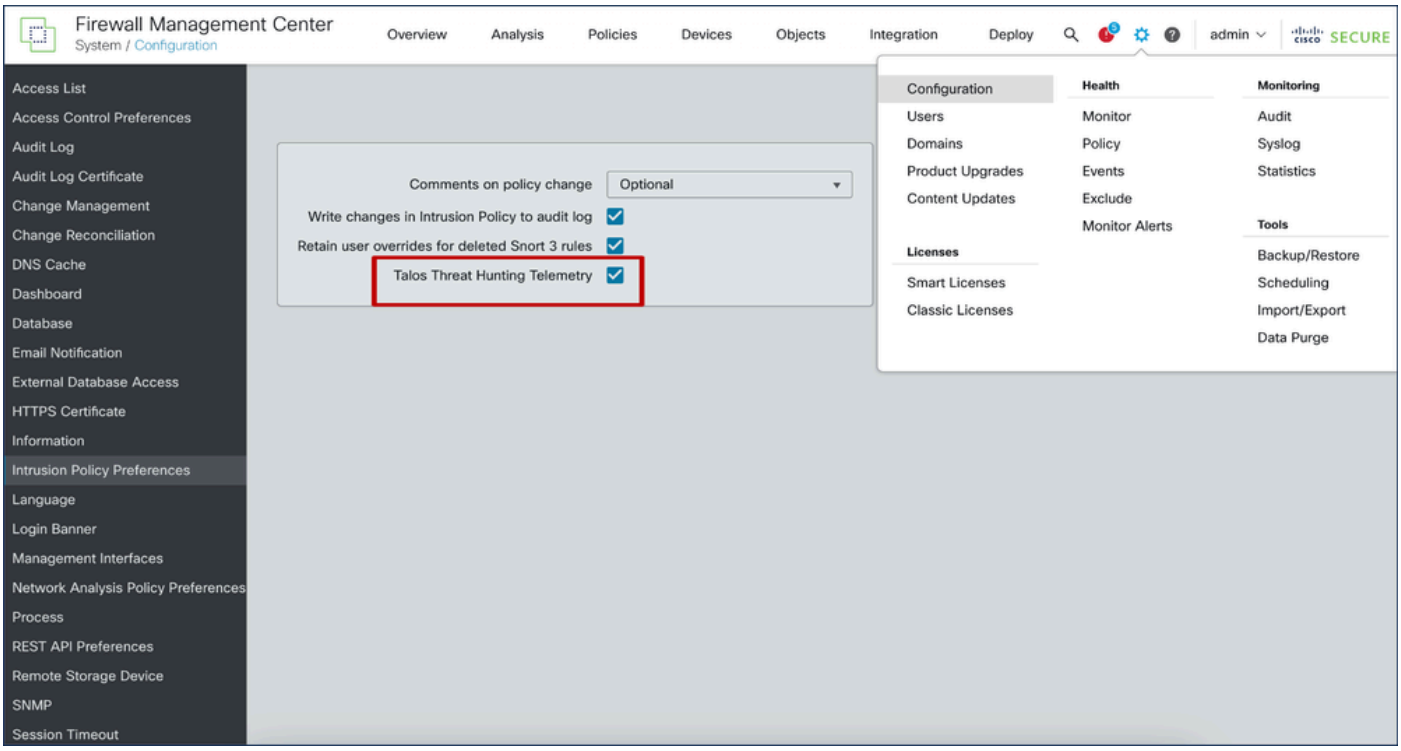
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

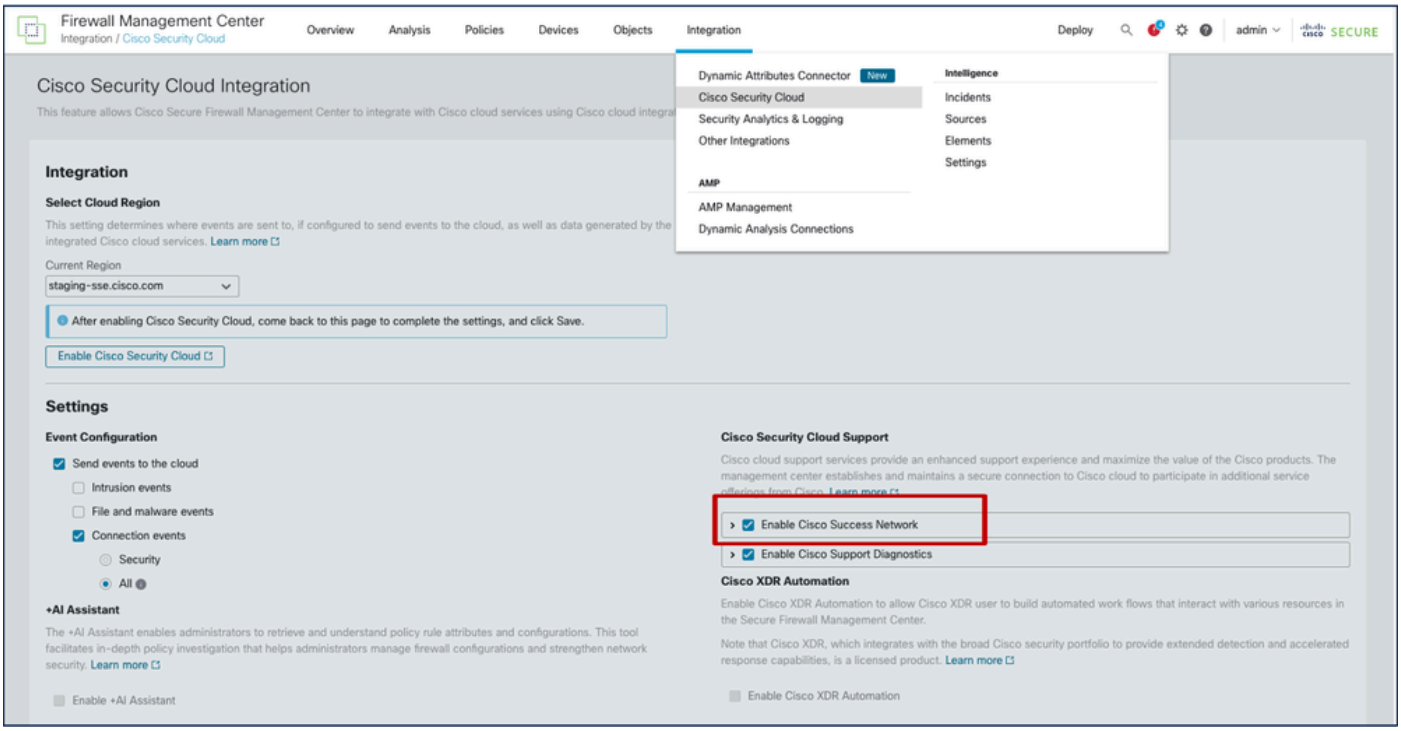
Detalhes do recurso

IU do FMC

- Caixa de seleção Novo sinalizador de recurso na página Sistema / Configuração / Preferência de política de intrusão para Telemetria de busca de ameaças do Talos.
- O sinalizador de recurso está ATIVADO por padrão, para novas instalações no 7.6.0 e para clientes existentes que estão atualizando para o 7.6.0.
- O recurso depende de "Enable Cisco Success Network". As opções "Enable Cisco Success Network" e "Talos Threat Hunting Telemetry" devem estar ativadas.
- Se ambos não estiverem ativados, o consumidor _SSE_ThreatHunting.json não será ativado e _SSE_ThreatHunting.json será necessário para processar e enviar os eventos para o Conector SSE.
- O valor do sinalizador de recurso é sincronizado com todos os dispositivos gerenciados com as versões 7.6.0 ou posterior.

Como funciona





- O sinalizador de recurso está armazenado em - /etc/sf/threat_hunting.conf no FMC.
- Esse valor de sinalizador de recurso também é salvo como "threat_hunt" em /var/sf/tds/cloud-events.json, que é sincronizado com dispositivos gerenciados em /ngfw/var/tmp/tds-cloud-events.json.
- Logs para verificar se o valor do sinalizador não é sincronizado com FTDs:
  - /var/log/sf/data_service.log no FMC.
  - /ngfw/var/log/sf/data_service.log no FTD.

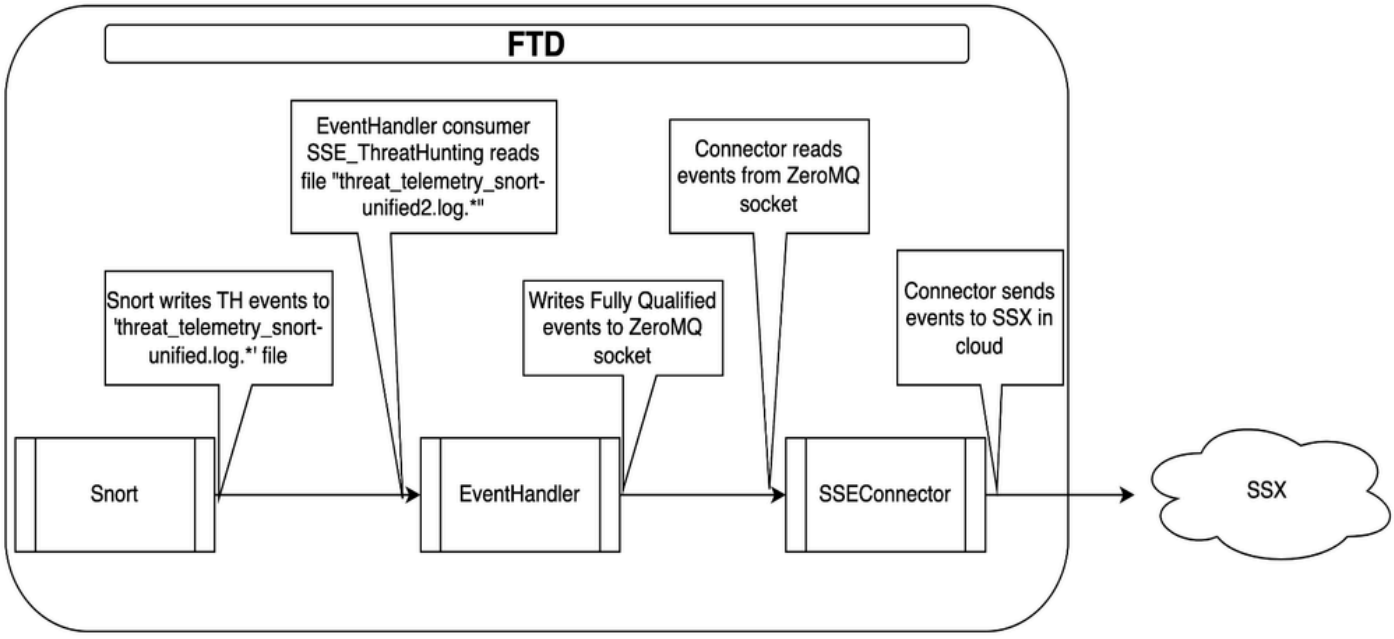
Snort 3

- As regras de Threat Hunting Telemetry (THT) são processadas da mesma forma que as regras comuns de IPS.
- FTD u2unified logger grava eventos de IPS de telemetria de busca de ameaças somente em threat_telemetry_snort-unified.log.*. Portanto, esses eventos não são visíveis para o usuário do FTD. O novo arquivo está localizado no mesmo diretório que snort-unified.log.*
- Além disso, os eventos de telemetria de busca de ameaças contêm um dump de buffers de IPS usados para avaliação de regras.
- Por ser uma regra de IPS, a regra de telemetria de busca de ameaças é um assunto para filtragem de eventos no Snort. No entanto, o usuário final não pode configurar event_filter para regras HTTP, pois elas não estão listadas no FMC.

Manipulador de eventos

- O Snort gera Intrusion, Packet e Extradataevents no prefixo de arquivo unificado threat_telemetry_snort-unified.log.*.
- EventHandler no dispositivo processa esses eventos e os envia para a nuvem através do conector SSX.
- Novo consumidor EventHandler para estes eventos:
  - /etc/sf/EventHandler/Consumers/SSE_ThreatHunting
  - Thread de baixa prioridade - É executado somente quando há CPU extra disponível

Como funciona



Troubleshooting

Troubleshooting de EventHandler - Dispositivo

- Procure logs EventHandler em /ngfw/var/log/messages

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

- Examine o arquivo /ngfw/var/log/EventHandlerStats para obter detalhes sobre o processamento de eventos:

```
{"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
```

- Se EventHandlerStats não mostrar eventos, verifique se o Snort está gerando eventos de busca de ameaças:

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

- Os eventos estão nos arquivos com o prefixo "threat_telemetry_snort-unified.log"
- Verifique os arquivos para os eventos desejados inspecionando esta saída:

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

- Se os arquivos não contiverem os eventos desejados, verifique:
  - Se a configuração do Threat hunt está habilitada
  - Se o Snortprocess está ou não em execução

Solução de problemas de configuração do Snort - Dispositivo

- Verifique se a configuração do Snort permite eventos de telemetria de busca de ameaças:

```
/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
```

- Verifique se as regras de telemetria de busca de ameaças estão presentes e habilitadas:

```
/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,"
```

- As regras de telemetria de busca de ameaças estão incluídas nas estatísticas de criação de perfil de regras. Portanto, se as regras consomem muito tempo de CPU, elas ficam visíveis nas estatísticas de criação de perfil da regra na página FMC.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.