Comprensión de la función de telemetría de Talos Threat Hunting en 7.6

Contenido

Introducción

Este documento describe la función Talos Threat Hunting Telemetry en 7.6.

Prerequisites

Requirements

Plataformas mínimas de software y 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

- Proporciona a Talos la capacidad de recopilar inteligencia y pruebas de falsos positivos mediante una clase especial de reglas que se aplican a los dispositivos Firepower.
- Estos eventos se envían a la nube a través del conector SSX y Talos los consume únicamente.
- Una nueva casilla de verificación que incluye las reglas de búsqueda de amenazas como parte de la configuración de la política global.
- Un nuevo archivo de registro (threat_telemetry_snort-unified.log.*) dentro del directorio instance-* para registrar los eventos de intrusión generados como parte de las reglas de

búsqueda de amenazas.
- Vuelca búferes IPS para las reglas de búsqueda de amenazas como un nuevo tipo de registro en datos adicionales.
- El proceso EventHandler utiliza un nuevo consumidor para enviar eventos IPS/Packet/Extradata a la nube en un formato totalmente calificado, empaquetado y comprimido.
- Estos eventos no se muestran en la IU de FMC

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

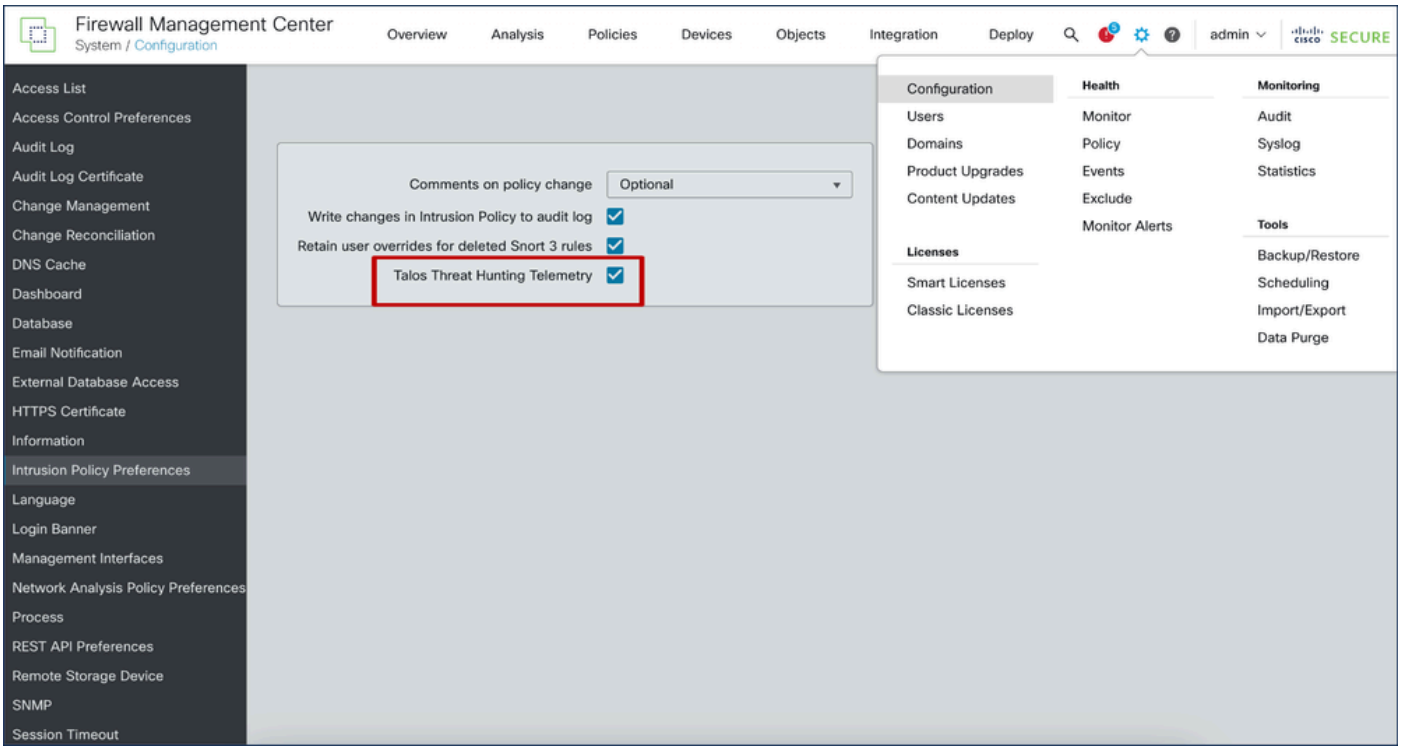
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

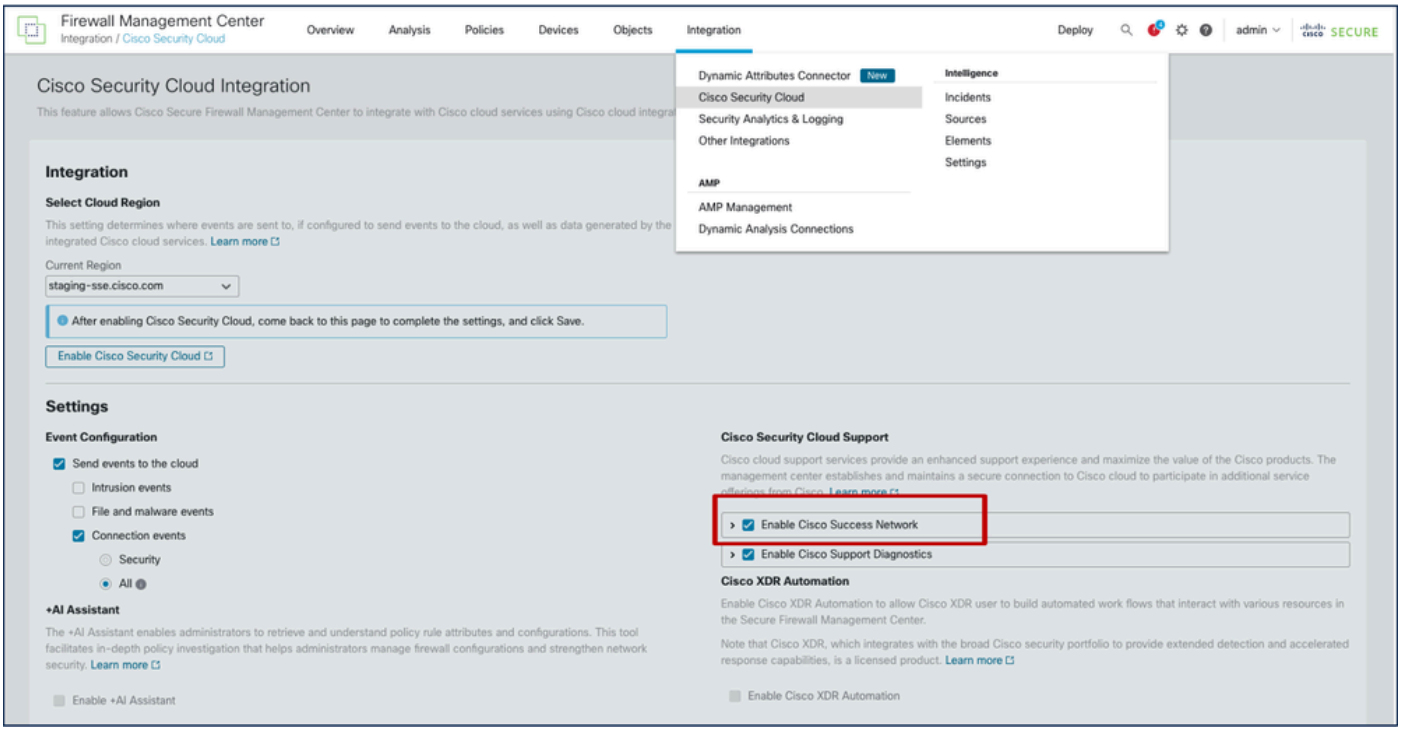
Detalles de la función

IU de FMC

- Casilla de verificación Nueva marca de función en la página Sistema / Configuración / Preferencia de política de intrusión para Talos Threat Hunting Telemetry.
- El indicador de la función está activado de forma predeterminada, tanto para las nuevas instalaciones en 7.6.0 como para los clientes existentes que actualizan a 7.6.0.
- Esta función depende de "Enable Cisco Success Network" (Habilitar red de éxito de Cisco). Deben activarse las opciones "Activar Cisco Success Network" y "Talos Threat Hunting Telemetry".
- Si no se habilitan ambos, el consumidor _SSE_ThreatHunting.json no se activa y se necesita _SSE_ThreatHunting.json para procesar y enviar los eventos al conector SSE.
- El valor del indicador de función se sincroniza con todos los dispositivos administrados con las versiones 7.6.0 o superiores.

Cómo funciona





- El indicador de función se almacena en - /etc/sf/threat_hunting.conf en FMC.
- Este valor del indicador de función también se guarda como "threat_ching" en /var/sf/tds/cloud-events.json, que se sincroniza con los dispositivos gestionados en /ngfw/var/tmp/tds-cloud-events.json.
- Registros para comprobar si el valor del indicador no se sincroniza con los FTD:
  - /var/log/sf/data_service.log en FMC.
  - /ngfw/var/log/sf/data_service.log en FTD.

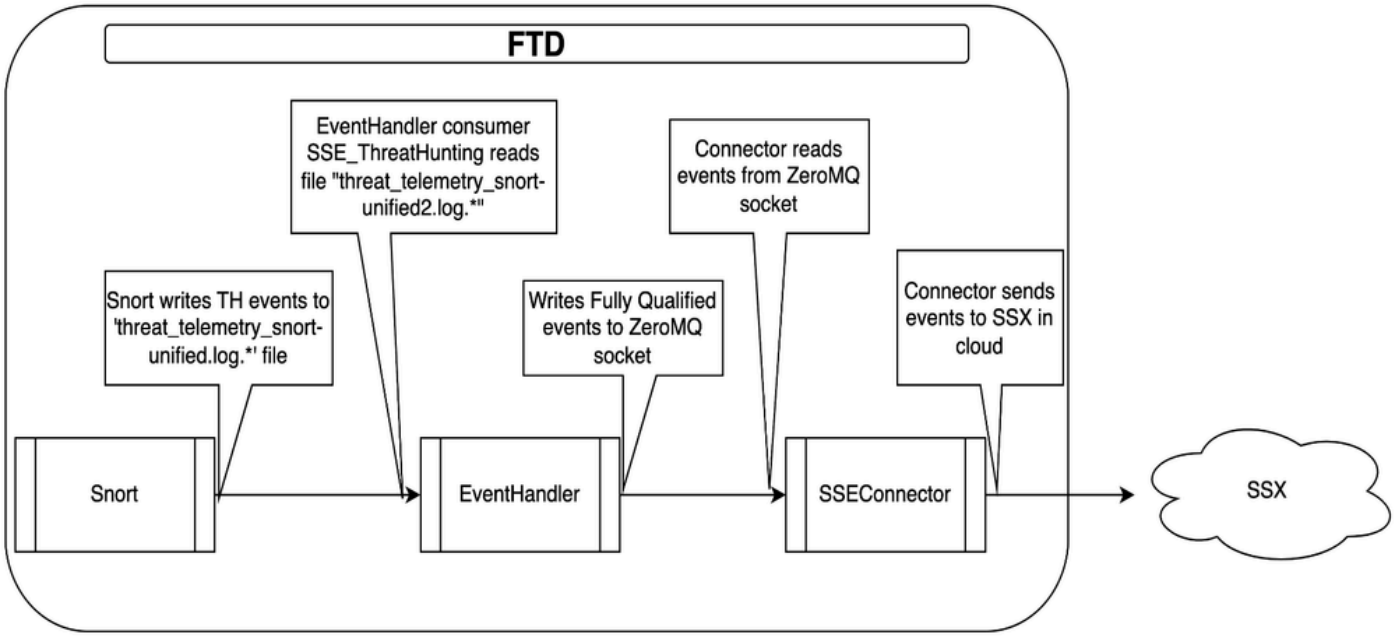
Snort 3

- Las reglas de telemetría de búsqueda de amenazas (THT) se procesan del mismo modo que las reglas IPS comunes.
- FTD u2unified logger escribe los eventos IPS de telemetría de búsqueda de amenazas solo en threat_telemetry_snort-unified.log.*. Por lo tanto, estos eventos no son visibles para el usuario de FTD. El nuevo archivo se encuentra en el mismo directorio que snort-unified.log.*
- Además, los eventos de telemetría de búsqueda de amenazas contienen un volcado de búferes IPS utilizados para la evaluación de reglas.
- Al ser una regla IPS, la regla de telemetría de búsqueda de amenazas es un asunto para el filtrado de eventos en el lado de Snort. Sin embargo, el usuario final no puede configurar event_filter para las reglas THT, ya que no aparecen en FMC.

Controlador de eventos

- Snort genera eventos de intrusión, paquete y extracción en el prefijo de archivo unificado threat_telemetry_snort-unified.log.*.
- EventHandler en el dispositivo procesa estos eventos y los envía a la nube a través del conector SSX.
- Nuevo consumidor de EventHandler para estos eventos:
  - /etc/sf/EventHandler/Consumers/SSE_ThreatHunting
  - Subproceso de baja prioridad: sólo se ejecuta cuando hay CPU adicional disponible

Cómo funciona



Resolución de problemas

Solución de problemas de EventHandler - Dispositivo

- Busque en /ngfw/var/log/messages los registros de EventHandler

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

- Busque los detalles del procesamiento de eventos en el archivo /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
```

- Si EventHandlerStats no muestra eventos, compruebe si Snort está generando eventos de búsqueda de amenazas:

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

- Los eventos se encuentran en los archivos con el prefijo "threat_telemetry_snort-unified.log"
- Verifique los archivos para los eventos deseados mediante la inspección de este resultado:

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

- Si los archivos no contienen los eventos deseados, compruebe:
  - Si la configuración de búsqueda de amenazas está o no habilitada
  - Si Snortprocess se está ejecutando o no

Resolución de problemas de configuración de Snort - Dispositivo

- Compruebe si la configuración de Snort habilita los eventos de telemetría de búsqueda de amenazas:

```
/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
```

- Compruebe si las reglas de telemetría de búsqueda de amenazas están presentes y 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,"
```

- Las reglas de telemetría de búsqueda de amenazas se incluyen en las estadísticas de generación de perfiles de reglas. Por lo tanto, si las reglas consumen mucho tiempo de

CPU, están visibles en las estadísticas de generación de perfiles de reglas en la página FMC.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).