了解7.6中的Talos威胁搜寻遥测功能

目录

简介

本文档介绍7.6中的Talos威胁搜寻遥感勘测功能。

先决条件

要求

最低软件和硬件平台

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

- 通过推送到Firepower设备的特殊规则类，为Talos提供收集情报和误报测试的能力。
- 这些事件通过SSX连接器发送到云，并且仅由Talos使用。
- 新功能复选框，其中包括作为全局策略配置一部分的威胁查找规则。
- instance-*目录内新的日志文件(threat_telemetry_snort-unified.log.*)，用于记录作为威胁搜索规则一部分生成的入侵事件。
- 将威胁搜索规则的IPS缓冲区转储为额外数据中的新记录类型。
- EventHandler进程使用新的使用者以完全限定格式（捆绑和压缩）将IPS/数据包/外部数据事件发送到云。
- FMC UI中不显示这些事件

使用的组件

本文档不限于特定的软件和硬件版本。

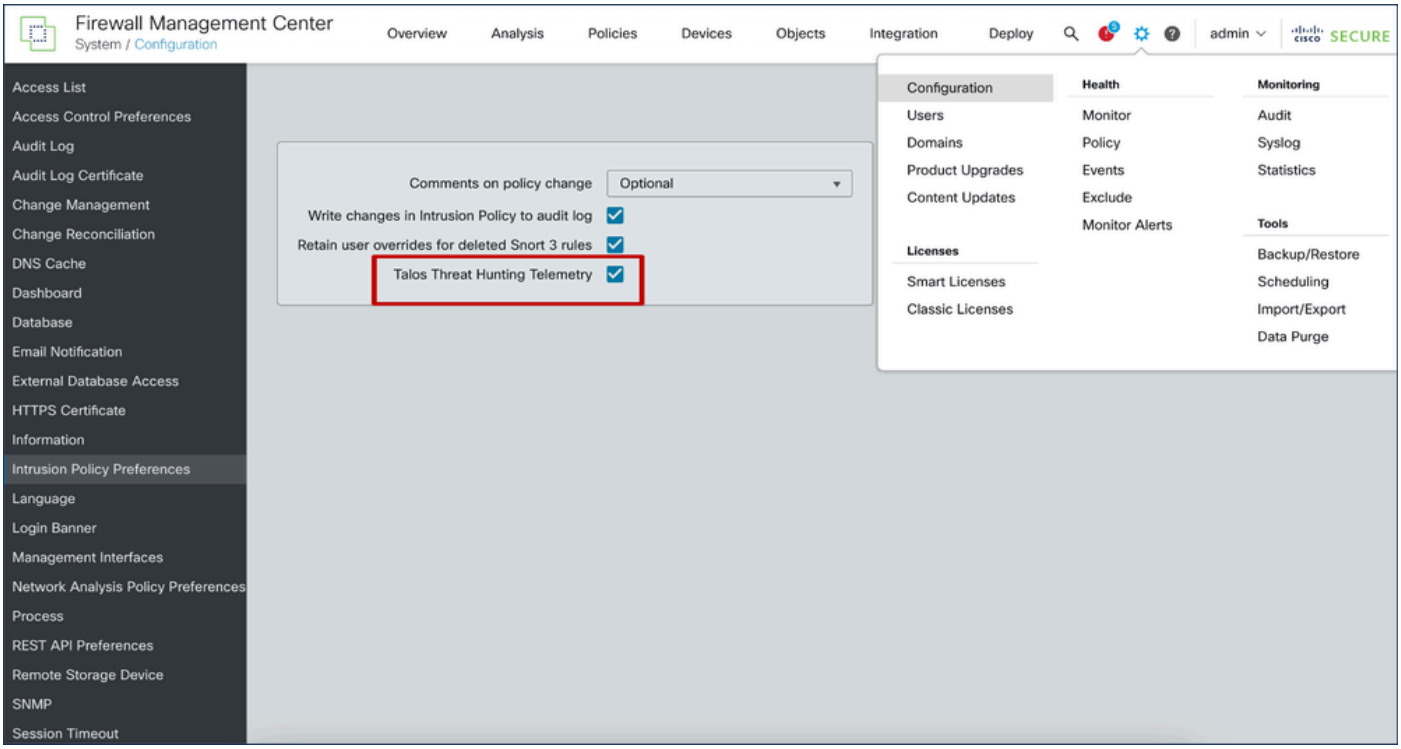
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

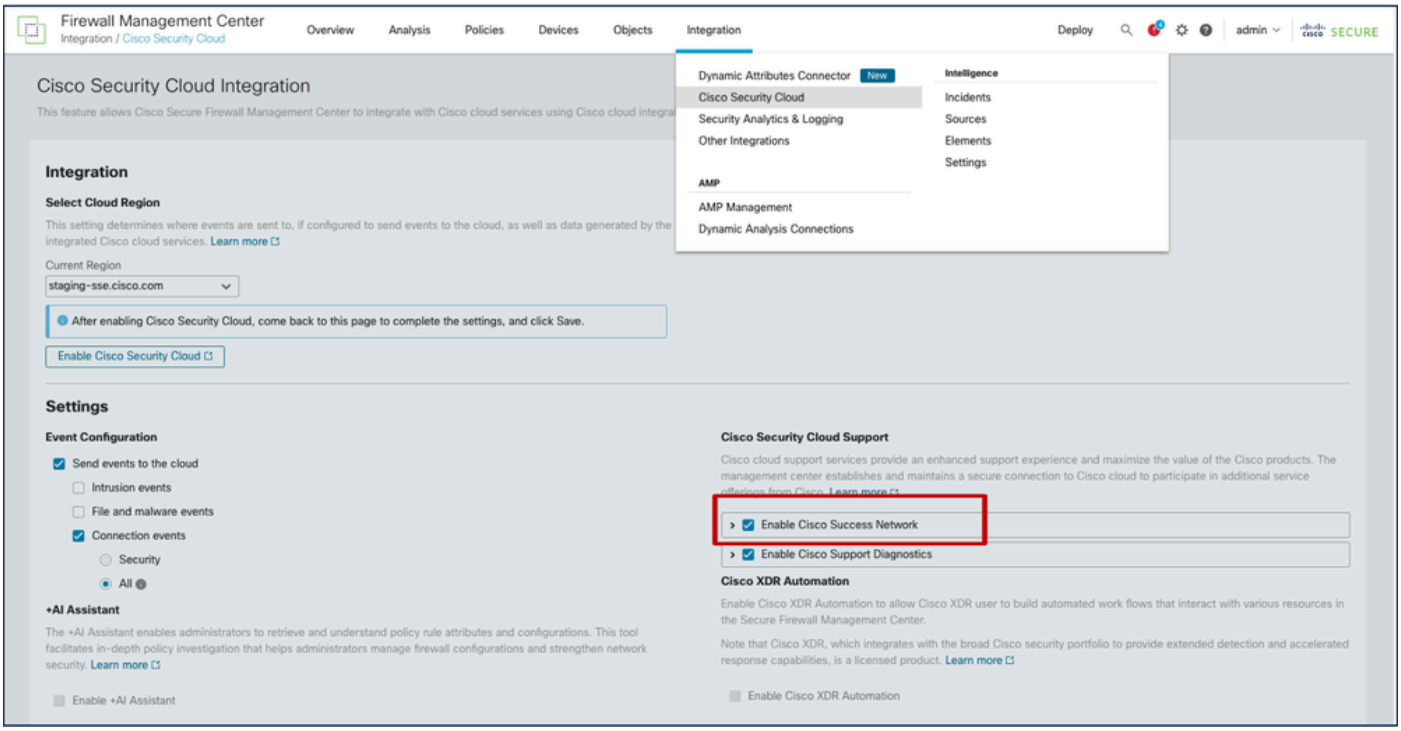
功能详细信息

FMC用户界面

- Talos威胁搜寻遥感勘测的系统/配置/入侵策略首选项页面上的新功能标志复选框。
- 对于7.6.0上的新安装以及升级到7.6.0的现有客户，功能标志默认打开。
- 功能依赖于“启用思科成功网络”。 必须同时启用“启用思科成功网络”和“Talos威胁搜寻遥测”选项。
- 如果两者均未启用，_SSE_ThreatHunting.json consumer不会打开，并且需要_SSE_ThreatHunting.json来处理事件并将其推送到SSE连接器。
- 功能标志值向下同步到版本为7.6.0或更高的所有受管设备。

工作原理





- 功能标志存储在FMC上的 — /etc/sf/threat_hunting.conf中。
- 此功能标志值也保存为/var/sf/tds/cloud-events.json中的“threat_hunting”，然后同步到/ngfw/var/tmp/tds-cloud-events.json上的受管设备。
- 日志以检查标记值是否未同步到FTD:
  - FMC上的/var/log/sf/data_service.log。
  - ftd上的/ngfw/var/log/sf/data_service.log。

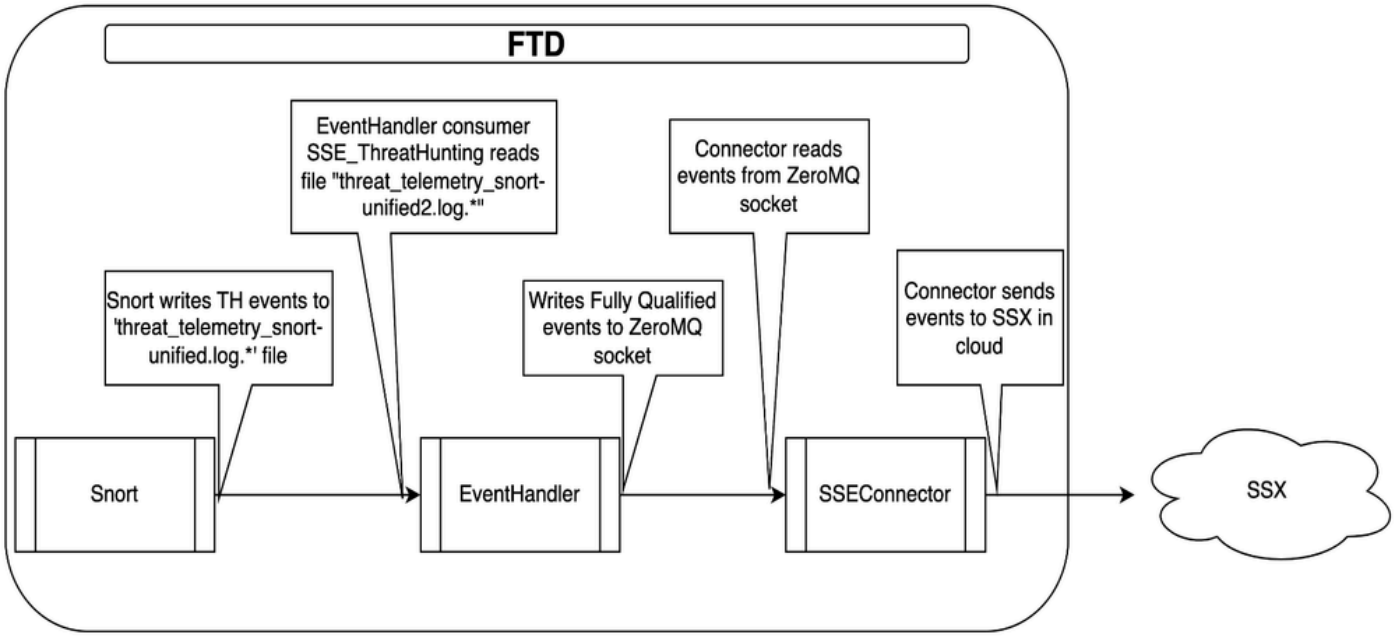
Snort 3

- 处理威胁搜寻遥测(THT)规则的方式与处理常见IPS规则的方式相同。
- FTD u2unified logger将威胁搜寻遥测IPS事件仅写入threat_telemetry_snort-unified.log.*。因此，这些事件对FTD用户不可见。新文件与snort-unified.log位于同一目录中。*
- 此外，威胁搜寻遥测事件包含用于规则评估的IPS缓冲区转储。
- 作为IPS规则，威胁搜寻遥测规则是Snort端事件过滤的主题。但是，最终用户无法为THT规则配置event_filter，因为它们未在FMC中列出。

事件处理程序

- Snort会在统一文件前缀threat_telemetry_snort-unified.log.*中生成入侵、数据包和提取事件。
- 设备上的EventHandler处理这些事件，并通过SSX连接器将它们发送到云。
- 这些事件的新EventHandler使用者：
  - /etc/sf/EventHandler/Consumers/SSE_ThreatHunting
  - 低优先级线程 — 仅在有额外CPU可用时运行

工作原理



故障排除

EventHandler故障排除 — 设备

- 在/ngfw/var/log/messages中查找EventHandler日志

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

- 在/ngfw/var/log/EventHandlerStats文件中查找事件处理详细信息：

```
{"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
```

- 如果EventHandlerStats未显示任何事件，则检查Snort是否正在生成威胁查找事件：

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

- 事件位于带有“threat_telemetry_snort-unified.log”前缀的文件中
- 通过检查以下输出检查所需事件的文件：

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

- 如果文件不包含所需事件，请检查：
  - 是否启用威胁查找配置
  - Snort进程是否正在运行

Snort配置故障排除 — 设备

- 检查Snort配置是否启用威胁搜寻遥测事件：

```
/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
```

- 检查是否存在并启用威胁搜索遥测规则：

```
/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,"
```

- 威胁搜寻遥测规则包含在规则分析统计信息中。因此，如果规则占用了大量CPU时间，则它们在FMC页面上的Rule Profiling统计信息中可见。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。