7.6의 Talos Threat Hunting 텔레메트리 기능 이해

목차

소개

이 문서에서는 7.6의 Talos 위협 헌팅 텔레메트리 기능에 대해 설명합니다.

사전 요구 사항

요구 사항

최소 소프트웨어 및 하드웨어 플랫폼

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

- Talos가 Firepower 디바이스에 푸시된 특수 클래스의 규칙을 통해 인텔리전스 및 오탐 테스트를 수집할 수 있는 기능을 제공합니다.
- 이러한 이벤트는 SSX 커넥터를 통해 클라우드로 전송되며 Talos에서만 소비됩니다.
- 전역 정책 컨피그레이션의 일부로 위협 헌팅 규칙이 포함된 새 기능 확인란.
- 위협 추적 규칙의 일부로 생성된 침입 이벤트를 로깅할 인스턴스-* 디렉토리 내의 새 로그 파일(threat_telemetry_snort-unified.log.*).
- 추가 데이터에서 위협 추적 규칙의 IPS 버퍼를 새 레코드 유형으로 덤프합니다.
- EventHandler 프로세스는 새로운 소비자를 사용하여 IPS/Packet/Extradata 이벤트를 번들형

및 압축된 정규화된 형식으로 클라우드에 전송합니다.
- 이러한 이벤트는 FMC UI에 표시되지 않습니다

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

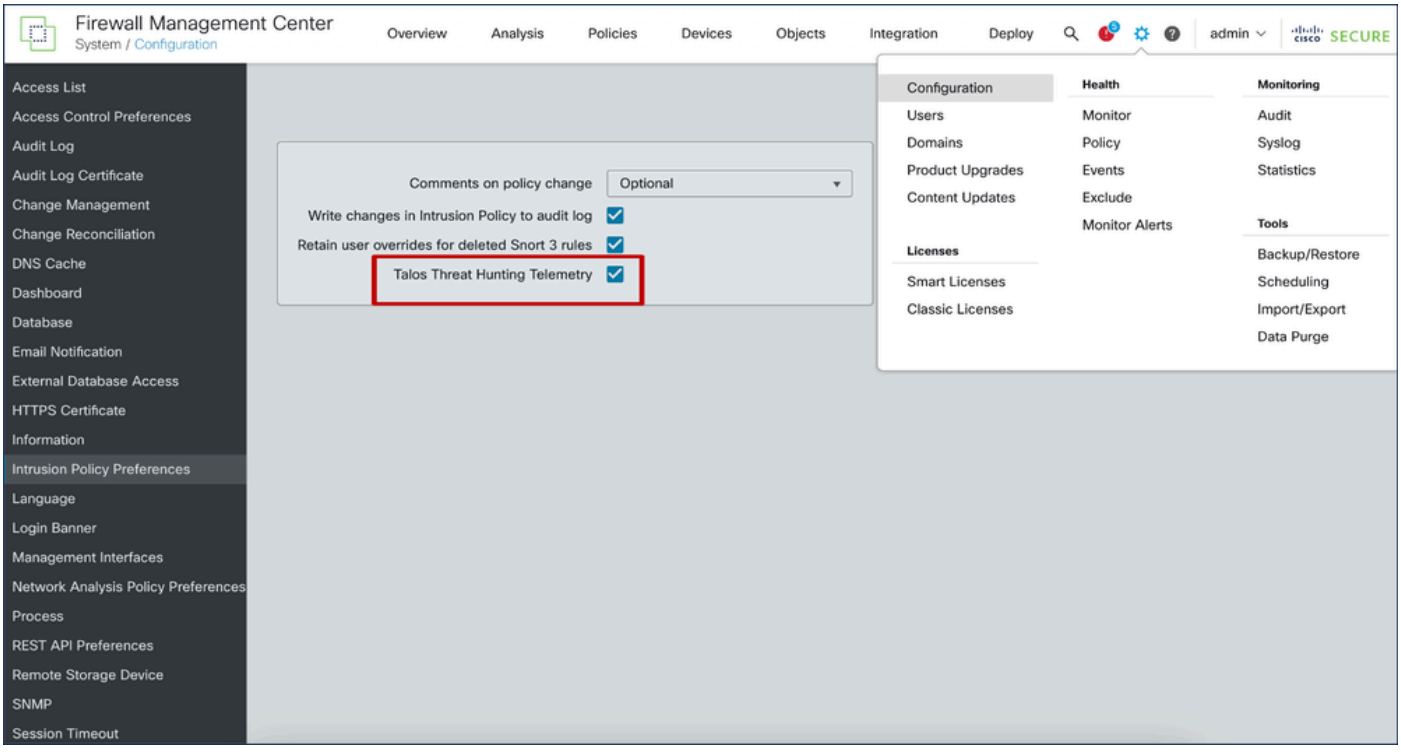
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

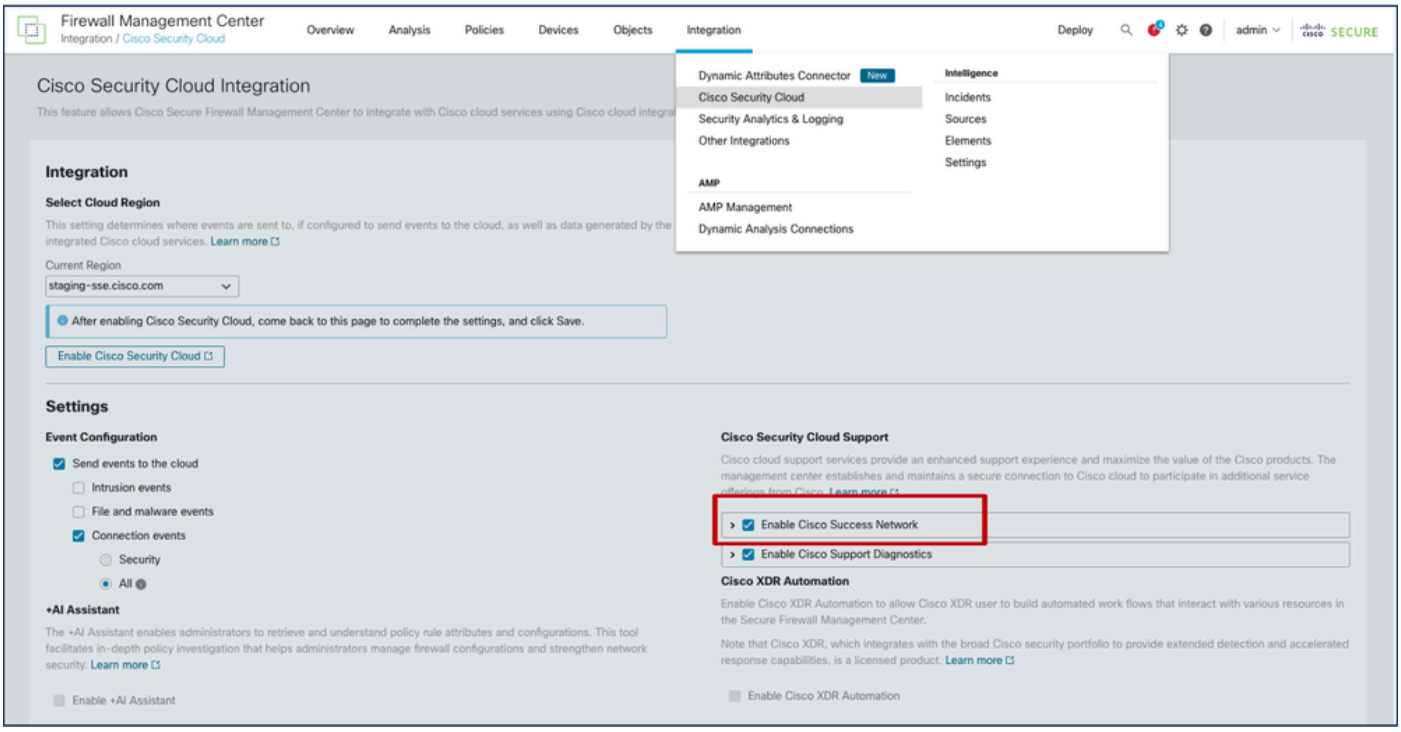
기능 세부사항

FMC UI

- Talos Threat Hunting Telemetry에 대한 System/Configuration/Intrusion Policy Preference(시스템/컨피그레이션/침입 정책 기본 설정) 페이지의 새 기능 플래그 확인란.
- 기능 플래그는 7.6.0에 새로 설치하는 경우와 7.6.0으로 업그레이드하는 기존 고객의 경우 모두 기본적으로 ON입니다.
- 이 기능은 "Cisco Success Network 활성화"에 종속됩니다. "Enable Cisco Success Network(Cisco 성공 네트워크 활성화)" 및 "Talos Threat Hunting Telemetry(Talos 위협 추적 텔레메트리)" 옵션을 모두 활성화해야 합니다.
- 둘 다 활성화되지 않은 경우 _SSE_ThreatHunting.json 소비자가 켜지지 않으며, 이벤트를 처리하고 SSE Connector로 푸시하려면 _SSE_ThreatHunting.json이 필요합니다.
- 기능 플래그 값은 버전 7.6.0 이상의 모든 관리되는 디바이스로 동기화됩니다.

운영 방식





- 기능 플래그는 FMC의 /etc/sf/threat_hunting.conf에 저장됩니다.
- 이 기능 플래그 값은 /var/sf/tds/cloud-events.json에서 "threat_hunting"으로 저장되며, 이는 /ngfw/var/tmp/tds-cloud-events.json에서 관리되는 디바이스로 동기화됩니다.
- 플래그 값이 FTD로 동기화되지 않았는지 확인하기 위한 로그:
  - FMC의 /var/log/sf/data_service.log
  - FTD의 /ngfw/var/log/sf/data_service.log입니다.

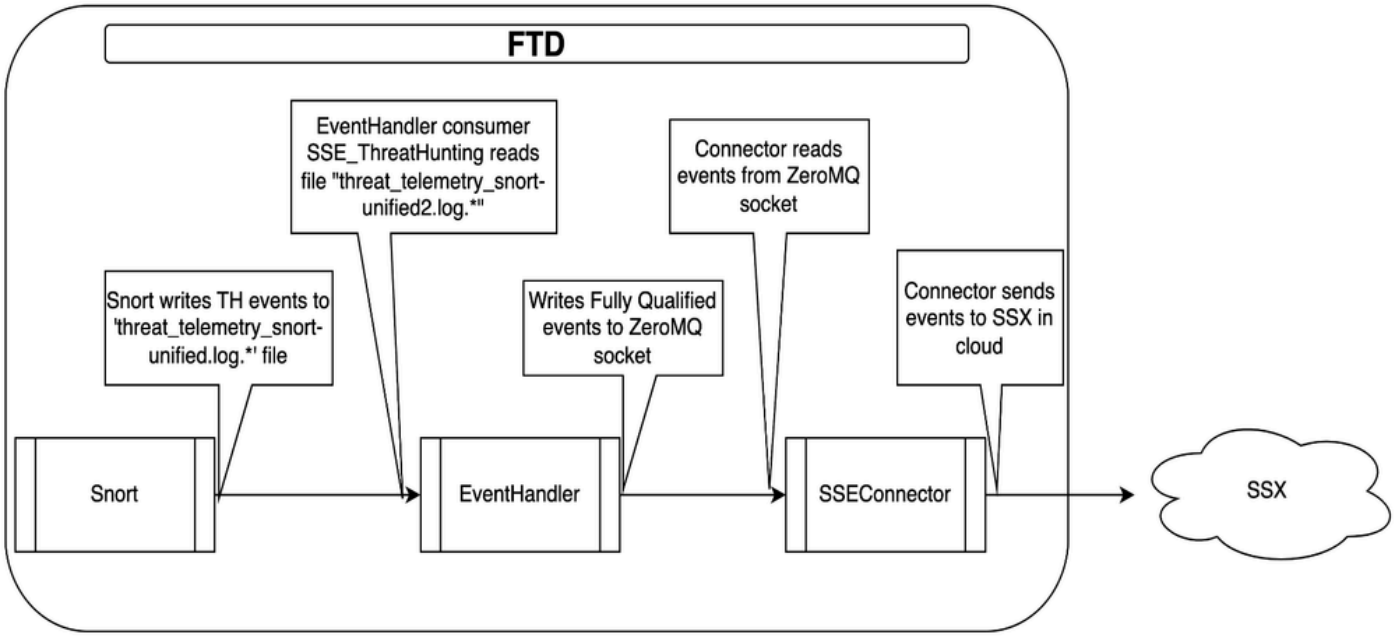
Snort 3

- THT(Threat Hunting Telemetry) 규칙은 일반 IPS 규칙과 동일한 방법으로 처리됩니다.
- FTD u2unified logger는 threat_telemetry_snort-unified.log에만 위협 헌팅 텔레메트리 IPS 이벤트를 기록합니다.* 따라서 FTD 사용자는 이러한 이벤트를 볼 수 없습니다. 새 파일은 snort-unified.log와 동일한 디렉토리에 있습니다.*
- 또한 위협 헌팅 텔레메트리 이벤트에는 규칙 평가에 사용되는 IPS 버퍼 덤프가 포함됩니다.
- IPS 규칙인 위협 헌팅 텔레메트리 규칙은 Snort 측의 이벤트 필터링에 적용됩니다. 그러나 THT 규칙은 FMC에 나열되지 않으므로 최종 사용자는 THT 규칙에 대해 event_filter를 구성할 수 없습니다.

이벤트 처리기

- Snort는 통합 파일 접두사 threat_telemetry_snort-unified.log.*에서 침입, 패킷 및 Extraataevents를 생성합니다.
- 장치의 EventHandler는 이러한 이벤트를 처리하고 SSX 커넥터를 통해 클라우드로 전송합니다.
- 다음 이벤트에 대한 새 EventHandler 소비자:
  - /etc/sf/EventHandler/Consumers/SSE_ThreatHunting
  - 낮은 우선 순위 스레드 - 추가 CPU를 사용할 수 있는 경우에만 실행됩니다.

운영 방식



문제 해결

EventHandler 문제 해결 - 장치

- /ngfw/var/log/messages에서 EventHandler 로그를 확인합니다.

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

- 이벤트 처리 세부 정보는 /ngfw/var/log/EventHandlerStats 파일을 참조하십시오.

```
{"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
```

- EventHandlerStats에 이벤트가 표시되지 않으면 Snort에서 위협 추적 이벤트를 생성하고 있는지 확인합니다.

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

- 이벤트는 "threat_telemetry_snort-unified.log" 접두사가 있는 파일에 있습니다
- 이 출력을 검사하여 원하는 이벤트에 대한 파일을 확인합니다.

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

- 파일에 원하는 이벤트가 포함되어 있지 않으면 다음을 선택합니다.
  - 위협 헌팅 컨피그레이션의 활성화 여부
  - Snortprocess의 실행 여부

Snort 컨피그레이션 트러블슈팅 - 디바이스

- Snort 컨피그레이션이 위협 헌팅 텔레메트리 이벤트를 활성화하는지 확인합니다.

```
/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
```

- 위협 헌팅 텔레메트리 규칙이 있고 활성화되었는지 확인합니다.

```
/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,"
```

- 위협 헌팅 텔레메트리 규칙은 규칙 프로파일링 통계에 포함되어 있습니다. 따라서 규칙이 CPU 시간을 많이 소비하는 경우 FMC 페이지의 Rule Profiling(규칙 프로파일링) 통계에 표시됩니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.