Comprendere la funzionalità di telemetria della caccia alle minacce Talos in 7.6

Sommario

Introduzione

Questo documento descrive la funzione di telemetria Talos Threat Hunting in 7.6.

Prerequisiti

Requisiti

Piattaforme software e hardware minime

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

- Fornisce funzionalità che consentono a Talos di raccogliere informazioni e test falsi positivi tramite una classe speciale di regole inviate ai dispositivi Firepower.
- Questi eventi vengono inviati al cloud tramite il connettore SSX e vengono utilizzati solo da Talos.
- Casella di controllo di una nuova funzionalità che include le regole di ricerca delle minacce come parte della configurazione dei criteri globali.
- Un nuovo file di log (threat_telemetry_snort-unified.log.*) all'interno della directory instance-* per registrare gli eventi di intrusione generati come parte delle regole di ricerca delle

minacce.
- Eseguire il dump dei buffer IPS per le regole di ricerca delle minacce come nuovo tipo di record nei dati aggiuntivi.
- Il processo EventHandler utilizza un nuovo consumer per inviare eventi IPS/Packet/Extradata al cloud in formato completo, in bundle e compresso.
- Questi eventi non vengono visualizzati nell'interfaccia utente di FMC

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

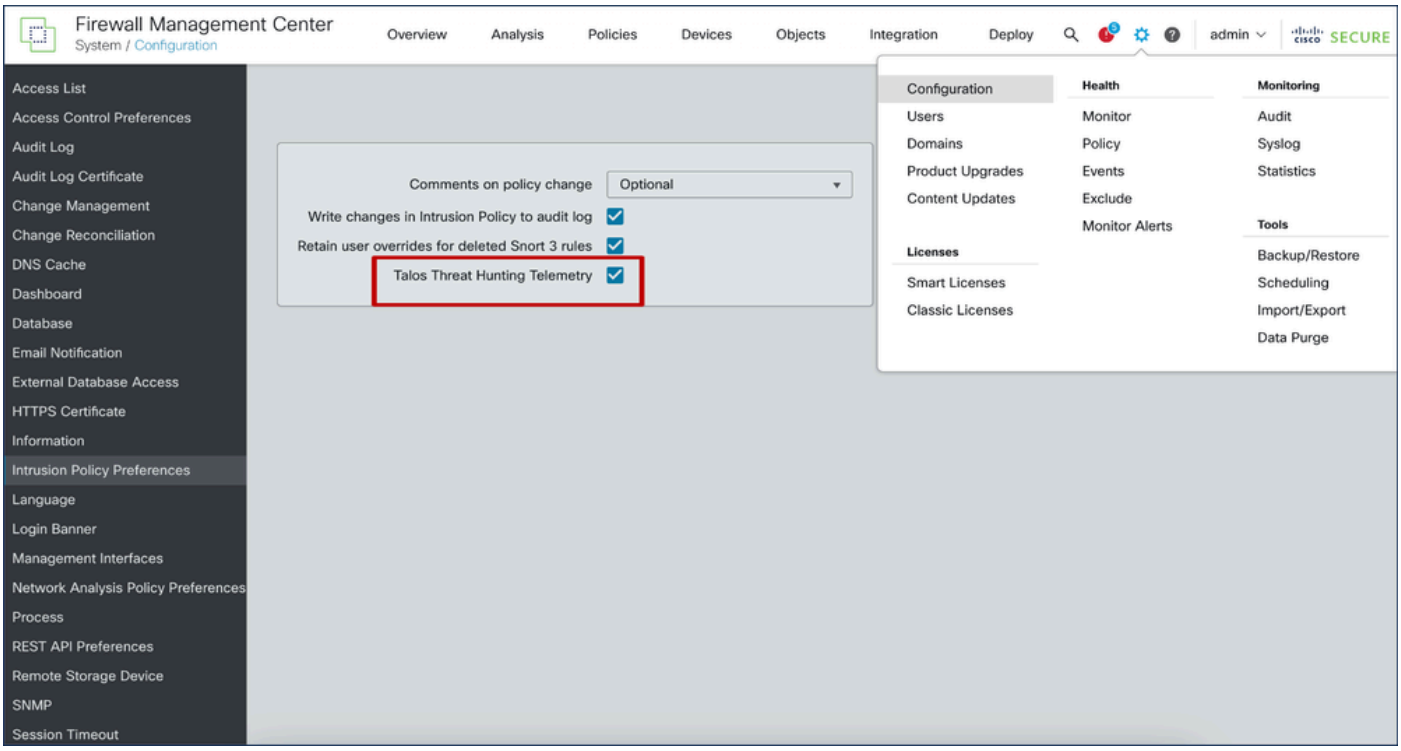
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

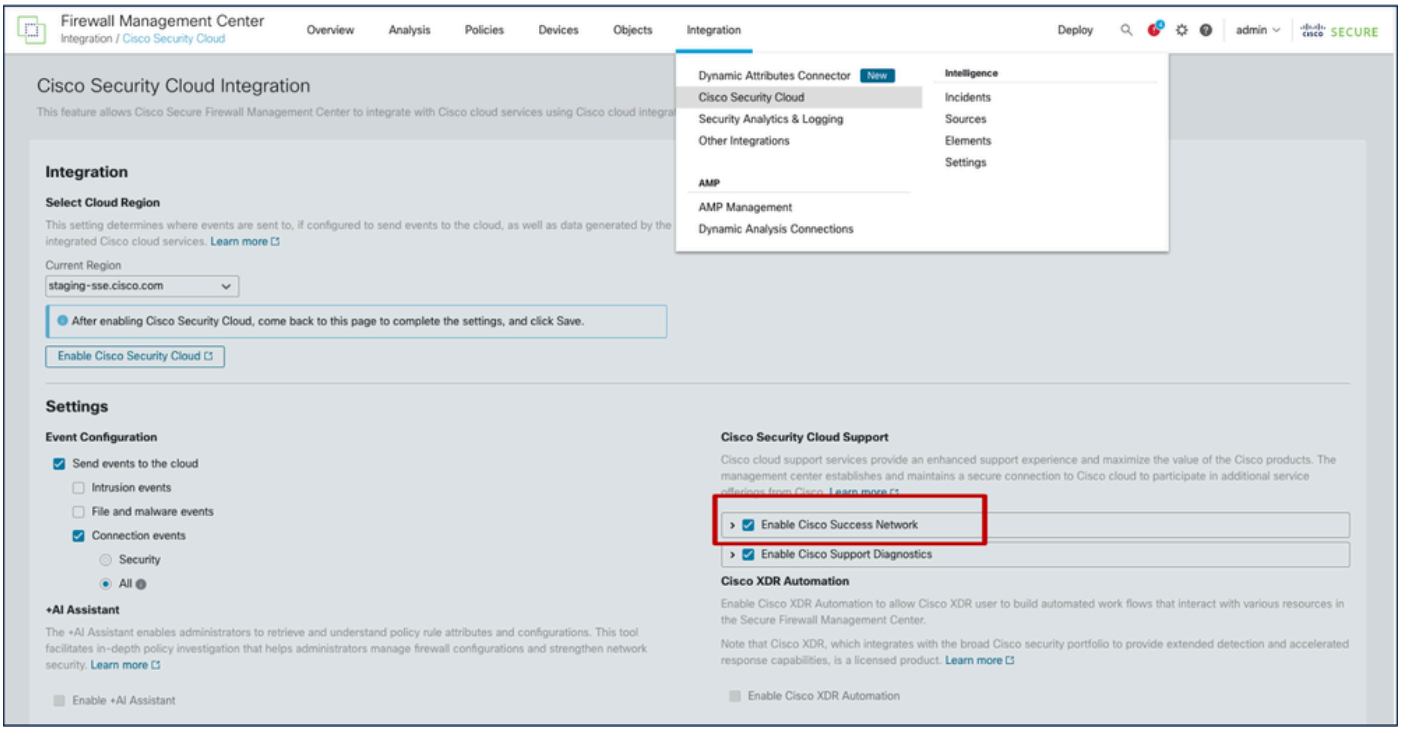
Dettagli funzionalità

Interfaccia utente FMC

- Casella di controllo Nuovo flag funzionalità nella pagina delle preferenze dei criteri di sistema/configurazione/intrusione per la telemetria Talos Threat Hunting.
- Il flag della funzionalità è ON per impostazione predefinita, sia per le nuove installazioni in 7.6.0 che per i clienti esistenti che eseguono l'aggiornamento a 7.6.0.
- Questa funzionalità dipende da "Abilita Cisco Success Network". È necessario abilitare entrambe le opzioni "Abilita Cisco Success Network" e "Telemetria di Talos Threat Hunting".
- Se non sono attivati entrambi, il consumer _SSE_ThreatHunting.json non si attiva e _SSE_ThreatHunting.json è necessario per elaborare e inviare gli eventi al connettore SSE.
- Il valore del flag della funzionalità viene sincronizzato con tutti i dispositivi gestiti con le versioni 7.6.0 o successive.

Come funziona





- Il flag della funzionalità è memorizzato in - /etc/sf/threat_hunting.conf su FMC.
- Il valore del flag della funzionalità viene salvato anche come "threat_hunting" in /var/sf/tds/cloud-events.json, che viene quindi sincronizzato con i dispositivi gestiti in /ngfw/var/tmp/tds-cloud-events.json.
- Registri per verificare se il valore del flag non viene sincronizzato con i FTD:
  - /var/log/sf/data_service.log sul CCP.
  - /ngfw/var/log/sf/data_service.log su FTD.

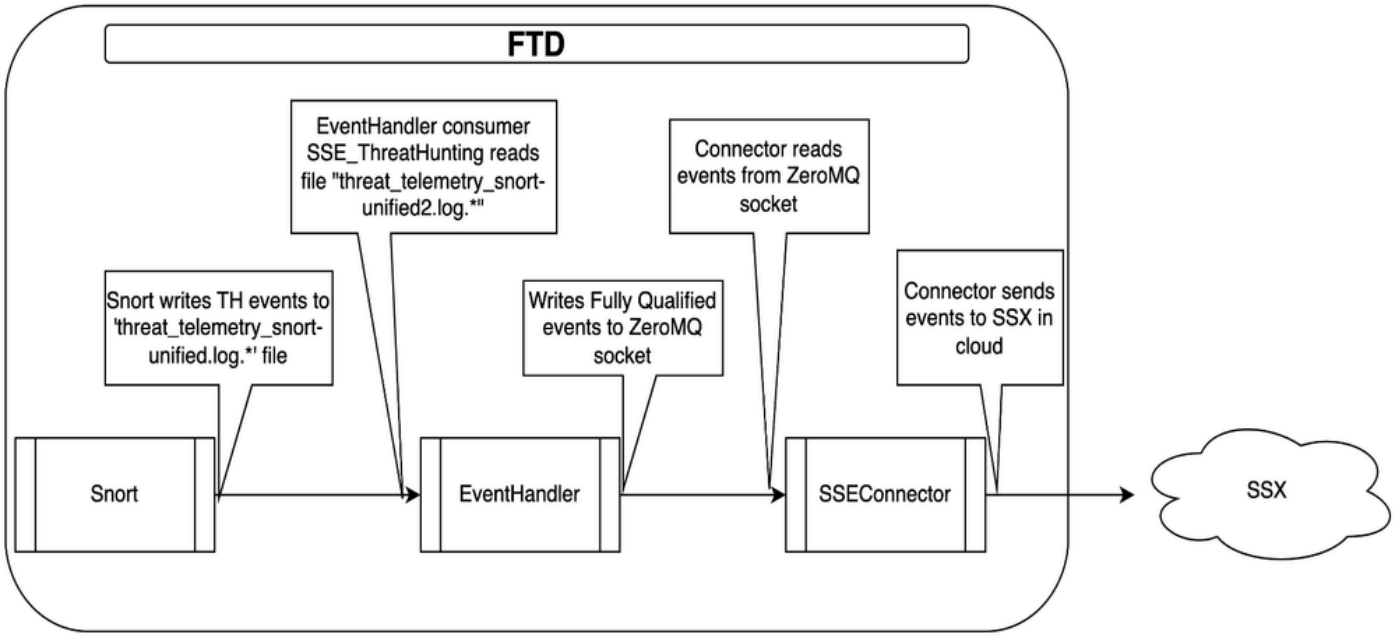
Snort. 3

- Le regole Threat Hunting Telemetry (THT) vengono elaborate allo stesso modo delle regole IPS comuni.
- FTD u2unified logger scrive eventi IPS di telemetria di caccia alla minaccia solo in threat_telemetry_snort-unified.log.*. Pertanto, questi eventi non sono visibili all'utente FTD. Il nuovo file si trova nella stessa directory di snort-unified.log.*
- Inoltre, gli eventi di telemetria per la ricerca di minacce contengono un dump dei buffer IPS utilizzati per la valutazione delle regole.
- Essendo una regola IPS, la regola di telemetria per la caccia alle minacce è un soggetto per il filtro degli eventi sul lato Snort. Tuttavia, l'utente finale non può configurare event_filter per le regole THT, poiché non sono elencate in FMC.

Gestore eventi

- Snort genera eventi Intrusion, Packet ed Extradatanel prefisso unificato threat_telemetry_snort-unified.log.*.
- EventHandler su dispositivo elabora questi eventi e li invia al cloud tramite il connettore SSX.
- Nuovo consumer EventHandler per questi eventi:
  - /etc/sf/EventHandler/Consumers/SSE_ThreatHunting
  - Thread a bassa priorità: viene eseguito solo quando è disponibile CPU aggiuntiva

Come funziona



Risoluzione dei problemi

Risoluzione dei problemi di EventHandler - Dispositivo

- Cercare i registri EventHandler in /ngfw/var/log/messages

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

- Per informazioni dettagliate sull'elaborazione degli eventi, cercare nel file /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
```

- Se EventHandlerStats non visualizza alcun evento, verificare se Snort sta generando eventi di ricerca di minacce:

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

- Gli eventi si trovano nei file con il prefisso "threat_telemetry_snort-unified.log"
- Controllare i file per gli eventi desiderati esaminando questo output:

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

- Se i file non contengono gli eventi desiderati, verificare:
  - Indica se la configurazione di Threat Caching è abilitata o meno
  - Indica se Snortprocess è in esecuzione

Risoluzione dei problemi relativi alla configurazione dello slot - Dispositivo

- Verificare se la configurazione Snort abilita gli eventi di telemetria di ricerca delle minacce:

```
/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_
```

- Verificare se le regole di telemetria per la caccia alle minacce sono presenti e abilitate:

```
/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,"
```

- Le regole di telemetria per la caccia alle minacce sono incluse nelle statistiche di profilatura delle regole. Pertanto, se le regole richiedono molto tempo di CPU, sono visibili nella pagina Statistiche di Profiling regole nella FMC.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).