تعرف على ميزة تتبع تتبع التهديد باستخدام نظام Talos في الإصدار 7.6

المحتويات

المقدمة

يصف هذا المستند ميزة "تتبع تتبع أثر تعقب تعقب تهديدات Talos" في 7.6.

المتطلبات الأساسية

المتطلبات

الحد الأدنى للبرامج والأجهزة الأساسية

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

- يوفر القدرة على جمع المعلومات الإستخباراتية والاختبارات الإيجابية المزيفة من خلال مجموعة خاصة من القواعد التي يتم دفعها إلى أجهزة الطاقة النارية.
- يتم إرسال هذه الأحداث إلى السحابة عبر موصل SSX، ويتم إستهلاكها بواسطة Talos فقط.
- خانة إختيار ميزة جديدة تتضمن قواعد البحث عن التهديدات كجزء من تكوين السياسة العالمية.
- يوجد ملف سجل جديد (threat_telemetry_snort-unified.log.*) داخل دليل instance-* لتسجيل أحداث الاختراق التي تنشأ كجزء من قواعد البحث عن التهديدات.

- قم بتفريغ المخازن المؤقتة لـ IPS لقواعد البحث عن التهديدات كنوع سجل جديد في البيانات الإضافية.
- تستخدم عملية EventHandler مستهلك جديد لإرسال أحداث IPS/Packet/Extradata إلى السحابة بتنسيق مؤهل بالكامل، ومضمن وضغوط.
- FMC مستخدم واجهة في هذه الأحداث التي تم عرضها

المكونات المستخدمة

هذا المستند على إصدارات برامج ومكونات مادية معينة.

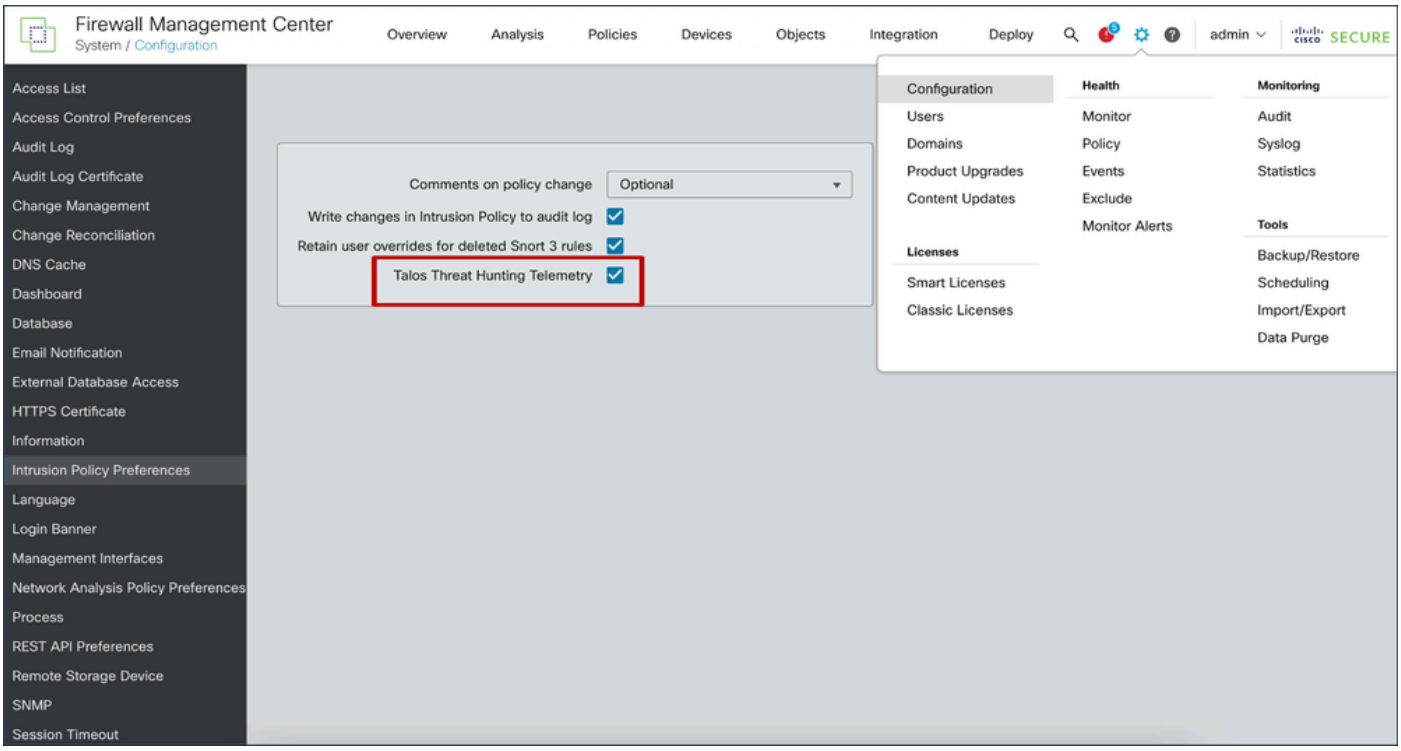
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

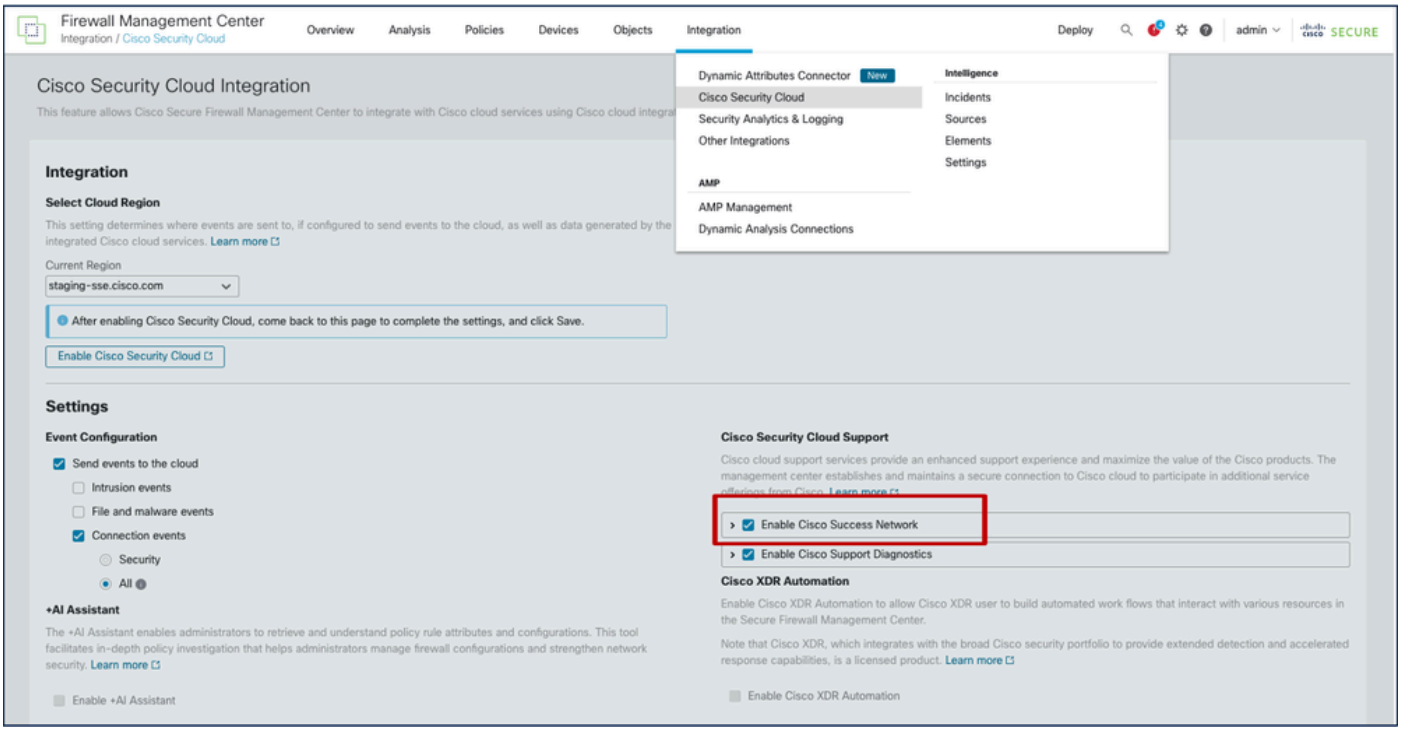
تفاصيل الميزة

مستخدم FMC واجهة

- قائمة إختيار عالمة ميزة جديدة في صفحة تفضيل نهج التطفل / التكوين / النظام لتصيد التهديدات بنظام Talos.
- تكون عالمة الميزة قيد التشغيل بشكل افتراضي، لكل من عمليات التثبيت الجديدة على 7.6.0 والمعلم الموجودين الذين يقومون بالترقية إلى 7.6.0.
- تعتمد الميزة على "تمكين شبكة نجاح Cisco". يجب تمكين كل من خيار "تمكين Telemetry" و"تتبع تتبع أخطاء البحث عن تهديدات شبكة نجاح Cisco".
- في حالة عدم تمكين الكل الطرازين، الموقع المستهلك_SSE_ThreatHunting.json لمعالجة الأحداث ودفعها إلى موصل SSE. يلزم وجود SSE_ThreatHunting.json، بالتشغيل
- تتزامن قيمة عالمة الميزة إلى جميع الأجهزة المدارة باستخدام الإصدار 7.6.0 أو إصدار أحدث.

كيف يعمل





- يتم تخزين علامة المميزة في - /etc/sf/threat_hunting.conf على FMC.
- يتم حفظ قيمة علامة المميزة هذه أيضا على أنها "threat_hunting" في /var/sf/tds/cloud-events.json، والذي يتم بعد ذلك مزامنته ووصوله إلى الأجهزة المدارة في /ngfw/var/tmp/tds-cloud-events.json.
- سجلات للتحقق مما إذا كانت قيمة العلامة ال تتزامن إلى FTDs:
  - /var/log/sf/data_service.log على FMC.
  - /ngfw/var/log/sf/data_service.log على FTD.

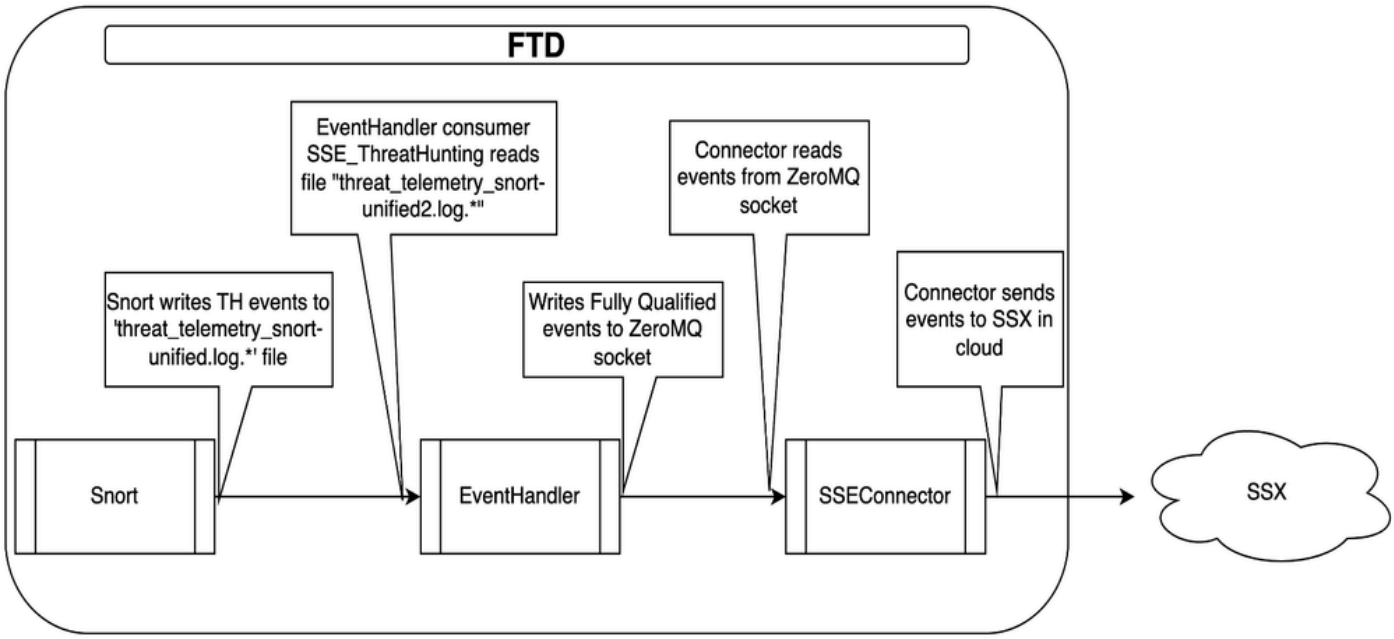
ورت 3

- تتم معالجة قواعد تتبع إستخدام مجموعات التهديدات (THT) بنفس الطريقة التي تتم بها معالجة قواعد IPS الشائعة.
- يكتب FTD U2Unified Logger أحداث IPS الخاصة بقياس التهديدات عن بعد فقط إلى THREAT_Telemetry_snort-unified.log.*. وبالتالي، فإن هذه الأحداث غير مرئية لمستخدم FTD. الملف الجديد موجود في نفس الدليل مثل snort-unified.log.*
- وبالإضافة إلى ذلك، تحتوي أحداث تتبع إستخدام التهديدات على تفريغ المخازن المؤقتة لنظام منع الاختراق (IPS) المستخدمة لتقييم القاعدة.
- وباعتبارها قاعدة لنظام منع الاختراق (IPS)، فإن قاعدة بيانات تتبع تتبع تتبع التهديدات هي موضوع لتصفية الأحداث على جانب الشرخ. ومع ذلك، لا يمكن للمستخدم النهائي تكوين event_filter لقواعد THT، لأنها غير مدرجة في FMC.

معالج الأحداث

- يولد Snort Intrusion و Packet و Extradataevents في بادئة الملف الموحدة threat_telemetry_snort-unified.log.*.
- يقوم EventHandler على الجهاز بمعالجة هذه الأحداث وإرسالها إلى السحابة عبر موصل SSX.
- مستهلك EventHandler الجديد لهذه الأحداث:
  - /etc/sf/EventHandler/Consumers/SSE_ThreatHunting
  - مؤشر ترابط منخفض الأولوية - يتم تشغيله فقط عند توفر وحدة المعالجة المركزية (CPU) الإضافية

كيف يعمل



استكشاف الأخطاء وإصلاحها

أستكشاف أخطاء معالج الأحداث وإصلاحها - الجهاز

- البحث في /ngfw/var/log/messages لسجلات EventHandler

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

- ابحث في ملف /ngfw/var/log/EventHandlerStats للحصول على تفاصيل معالجة الحدث:

```
{"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
```

- إذا لم يظهر EventHandlerStats أية أحداث، فتحقق مما إذا كان Snort يقوم بإنشاء أحداث البحث عن تهديدات:

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

- الأحداث موجودة في الملفات باستخدام البادئة "threat_telemetry_snort-unified.log"
- تحقق من الملفات للأحداث المطلوبة عن طريق فحص هذا الإخراج:

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

- إذا لم تحتوي الملفات على الأحداث المطلوبة، فتحقق من:
  - ما إذا تم تمكين تكوين البحث عن التهديدات أم لا
  - ما إذا كان Snortprocess قيد التشغيل أم لا

استكشاف أخطاء تكوين الجهاز وإصلاحها

- التحقق مما إذا كان تكوين SNORT يمكن أحداث تتبع تتبع تعقب التهديدات:

```
/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
```

- تحقق مما إذا كانت قواعد تتبع تتبع تتبع تتبع عملية البحث عن التهديدات موجودة ومكنة أم ال:

```
/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,"
```

- يتم تضمين قواعد تتبع تتبع عمليات البحث عن التهديدات في إحصائيات تحديد سمات القواعد. لذا، فإذا استهلكت القواعد قدرا كبيرا من وقت وحدة المعالجة المركزية، فإنها تصبح مرئية في إحصائيات تحديد سمات القواعد على صفحة وحدة المعالجة المركزية (FMC).

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).