أستكشاف أخطاء تكامل FMC مع CTR وإصلاحها

المحتويات

المقدمة

يصف هذا المستند الخطوات الرامية إلى أستكشاف أخطاء عملية موصل تبادل خدمات الأمان (SSE) وإصلاحها عند تعطيلها على مركز إدارة FirePOWER (FMC) أو أجهزة الدفاع عن تهديد FirePOWER (FTD) للتكامل مع الاستجابة لتهديدات Cisco (CTR).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- FMC
- نظام Firepower Threat Defense (FTD)
- تكامل CTR

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- FMC على برنامج الإصدار 6.4.0 أو إصدار أعلى

- برنامج FTD على الإصدار 6.4.0 أو إصدارا أعلى
- تبادل خدمات الأمان من Cisco
- حساب CTR

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

معلومات أساسية

شركة SsecConnector

SSEContor هي عملية على أجهزة FirePOWER بعد 6.4.0 تقوم بتسجيل الأجهزة في بوابة SSE. تقوم FMC بالبث إلى جميع FTDs المدارة عند تعييني تكوين سحابة Cisco على تشغيل وأو إيقاف التشغيل. بمجرد تمكين سحابة Cisco، تبدأ خدمة SSEContor الاتصال بين مدخل SSE وأجهزة FirePOWER. يطلب كل FTD من FMC الحصول على رمز مميز للتسجيل يسمح بدمج الأجهزة في بوابة SSE. بعد هذا التكامل، يتم تنشيط سياق SSE على الأجهزة ويعاد تكوين EventHandler لإرسال أحداث الاقتحام إلى سحابة Cisco.

تشتر

الاستجابة للتهديدات هي مركز تنسيق الاستجابة لحوادث التهديدات، والذي يدعم وأتمتة عمليات التكامل عبر منتجات أمان متعددة من Cisco. تعمل الاستجابة للتهديدات على تسريع المهام الأمنية الأساسية: الكشف والتحقيق والمعالجة، وهي حجر الزاوية في بنيتنا الأمنية المتكاملة.

إن الهدف من ميزة "الاستجابة للتهديدات" هو مساعدة فرق عمليات الشبكة والمستجيبين للحوادث على فهم التهديدات على شبكتهم بواسطة جميع المعلومات الإستخباراتية الخاصة بالتهديد التي تم جمعها وجمعها والتي توفرها Cisco وأطراف أخرى.

لكن الهدف من الإستجابة للتهديدات هو القلل من تعقيد الأدوات الأمنية، والمساعدة على التعرف على التهديدات، وتسريع الإستجابة للحوادث.

الاستجابة للتهديدات هي منصة للتكامل (https://visibility.amp.cisco.com/). يعمل النظام عبر "وحدات"، وهي أجزاء مستقلة من التعليمات البرمجية التي تتعامل مع الاتصالات مع أنظمة مدمجة مختلفة (مثل شبكة الحماية أو AMP). وتتولى هذه الوحدات كل الوظائف الثلاث التي يستطيع النظام المتكامل أن يوفرها (الإثراء، والسياق المحلي، والاستجابة).

ما الذي يمكن إستخدام CTR فيه؟

- الإستجابة للحدث
- التحقيقات
- صيد التهديدات
- إدارة الحوادث

عندما تبحث عن جهاز يمكن ملاحظته، فإن جميع الوحدات التي قمت بتكوينها تسأل الأنظمة التي تكون مسؤولة عن البحث عن أي سجل لهذه الأجهزة المرفقة. ثم يقومون بعد ذلك بأخذ الردود المقدمة وإعادتها إلى إستجابة التهديد، ثم يقوم بأخذ النتائج التي تم تجميعها من جميع الوحدات التعليمية (في هذه الحالة وحدة Stealthwatch)، ويقوم بفرز وتنظيم البيانات وعرضها في رسومة بيانية.

لدمج CTR مع منتجات مختلفة، هناك بوابتان إضافيتان هما https://castle.amp.cisco.com/"

(Castle) وhttps://admin.sse.itd.cisco.com/app/devices" (تبادل خدمات الأمان)

بوابة القلعة

هنا يمكنك إدارة حسابات أمان Cisco:

يسمح لكل حساب أمان Cisco بإدارة تطبيقات متعددة داخل مجموعة أمان Cisco. وفقا لمستحقات الترخيص الخاصة بك، يمكن أن تتضمن هذا ما يلي:

- AMP لنقاط النهاية
- شبكة تهديدات
- الإستجابة للتهديدات

بوابة تبادل خدمات الأمان

تعد هذه البوابة امتدادا لبوابة CTR، حيث يمكنك إدارة الأجهزة التي تم تسجيلها في بوابة CTR، وبالتالي يمكنك هنا إنشاء العلامات المميزة المطلوبة لدمج المنتجات.

يوفر تبادل خدمات الأمان إدارة الأجهزة والخدمات والأحداث عند دمج بعض منتجات الأمان من Cisco مع ميزة "الاستجابة لتهديدات Cisco"، بما في ذلك هذه المنتجات والميزات:

- إدارة قائمة أجهزة إدارة الأمان التي تتكامل مع إستجابة تهديدات Cisco.
- قم بجمع بيانات الحدث من أجهزة FirePOWER المدمجة من Cisco، إستعداد لإعادة توجيهها (تلقائيا أو يدويا) إلى إستجابة تهديد Cisco.

استكشاف الأخطاء وإصلاحها

التحقق من تمكين خدمات السحابة

في FMC، أولا، تحقق من **التراخيص>النظام>التراخيص>التراخيص الذكية** لست في وضع التقييم.

تحقق الآن ضمن **النظام>التكامل** على علامة التبويب **القرص الصناعي للبرامج الذكية** أن الخيار المحدد هو **الاتصال مباشرة بمدير البرنامج الذكي من Cisco** حيث أن هذه الميزة غير مدعومة على بيئة محولة وائيا.

انتقل إلى **النظام >التكامل** على علامة التبويب **خدمات السحابة** وتحقق من تشغيل خيار **تكوين حدث سحابة Cisco**.

التحقق من الاتصال بين بوابة FMC/FTD و SSE

يجب السماح بعنوان URLs التالي كما يمكن أن تتغير عناوين IP:

المنطقة الامريكية

- api-sse.cisco.com
- est.sco.cisco.com (شائع عبر جغرافيا)
- mx*.sse.itd.cisco.com (حاليا mx01.sse.itd.cisco.com فقط)

- dex.sse.itd.cisco.com (لنجاح العملاء)
- eventing-ingest.sse.itd.cisco.com (ل CTR و CDO)

منطقة الاتحاد الأوروبي

- api.eu.sse.itd.cisco.com
- est.sco.cisco.com (شائع عبر جغرافي)
- mx*.eu.sse.itd.cisco.com (حالي mx01.eu.sse.itd.cisco.com فقط)
- dex.eu.sse.itd.cisco.com (لنجاح العملاء)
- eventing-ingest.eu.sse.itd.cisco.com (ل CTR و CDO)

منطقة آسيا والمحيط الهادئ واليابان

- api.apj.sse.itd.cisco.com
- est.sco.cisco.com (مشتركة عبر المسافات الجغرافية)
- mx*.apj.sse.itd.cisco.com (حالي mx01.apj.sse.itd.cisco.com فقط)
- dex.apj.sse.itd.cisco.com (لنجاح العملاء)
- eventing-ingest.apj.sse.itd.cisco.com (بالنسبة للجنة مكافحة الإرهاب واتفاقية حقوق الأشخاص ذوي الإعاقة)

يحتاج كل من FMC و FTD إلى اتصال بعنوان SSE URLs على واجهة الإدارة الخاصة بهما، لاختبار الاتصال، أدخل هذه الأوامر على Firepower CLI مع الوصول الجذر:

```
curl -v https://api-sse.cisco.com/providers/sse/services/registration/api/v2/clients --cacert
/ngfw/etc/ssl/connectorCA.pem
curl -v https://est.sco.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem

curl -v https://eventing-ingest.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
curl -v https://mx01.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

بعد تشغيل كل أمر، يجب أن ترى هذا السطر حول نهاية الاتصال: **الاتصال #0 لاستضافة "URL" تركت البر تغيير**.

إذا انتهت مهلة الاتصال أو لم تستلم هذا السطر على الإخراج، فالرجاء التحقق من أن واجهات الإدارة مسموح لها بالوصول إلى عناوين URL هذه ومن عدم وجود أجهزة للتحميل تمنع الاتصال بين الأجهزة وعناوين URL هذه أو تعدله.

يمكن تجاوز التحقق من الشهادة بهذا الأمر:

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying 52.4.85.66...
* Connected to api-sse.cisco.com (52.4.85.66) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: none
CApath: /etc/ssl/certs
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Request CERT (13):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
```

```
* TLSv1.2 (OUT), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api -sse.cisco.com
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID S SL ICA G2
* SSL certificate verify result: self signed certificate in certificate c hain (19), continuing
anyway.
>GET / HTTP/1.1
>Host: api-sse.cisco.com
>User-Agent: curl/7.44.0
>Accept: */*
>
<HTTP/1.1 403 Forbidden
<Date: Wed, 08 Apr 2020 01:27:55 GMT
<Content-Type: text/plain; charset=utf-8
<Content-Length: 9
<Connection: keep-alive
<Keep-Alive: timeout=5
<ETag: "5e17b3f8-9"
<Cache-Control: no-store
<Pragma: no-cache
<Content-Security-Policy: default-src 'self'
<X-Content-Type-Options: nosniff
<X-XSS-Protection: 1; mode=block
<Strict-Transport-Security: max-age=31536000; includeSubdomains;
```

ةظحالم: يمكنك الحصول على الرسالة 403 المحظورة لأن المعلومات التي تم إرسالها من الاختبار ليست مشفرة SSE ولكن هذا يثبت بما يكفي للتحقق من الاتصال.

التحقق من حالة SsecConnector

يمكنك التحقق من خصائص الموصل كما هي أدناه.

```
# more /ngfw/etc/sf/connector.properties
registration_interval=180
connector_port=8989
connector_fqdn=api-sse.cisco.com
```

للتحقق من الاتصال بين SSContor و EventHandler الذي يمكنك إستخدام هذا الأمر، هذا مثال على اتصال سيئ:

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 3022791165 11204/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.sock
```

في مثال على اتصال ثابت، يمكنك أن ترى أن حالة المقبس متصلة:

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 382276 7741/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.sock
```

```
unix 3 [ ] STREAM CONNECTED 378537 7741/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.soc
```

التحقق من البيانات المرسلة إلى بوابة SSE و CTR

للإسال أحداث من جهاز FTD للاطلاع على حالة إنشاء اتصال TCP مع https://eventing-ingest.sse.itd.cisco.com هذا مثال على اتصال لم يتم إنشاؤه بين مدخل SSE و FTD:

```
root@firepower:/ngfw/var/log/connector# lsof -i | grep conn
connector 60815 www 10u IPv4 3022789647 0t0 TCP localhost:8989 (LISTEN)
connector 60815 www 12u IPv4 110237499 0t0 TCP firepower.cisco.com:53426->ec2-100-25-93-
234.compute-1.amazonaws.com:https (SYN_SENT)
```

في الموصل.السجلات:

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 18.205.49.246:443: getsockopt: connection timed out"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 18.205.49.246:443: getsockopt: connection timed out"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
```

> **ملاحظة**: لاحظ أن عنواني IP المعروضة 18.205.49.246 و 18.205.49.246 تنتمي إلى https://eventing-ingest.sse.itd.cisco.com قد تتغير، ولهذا السبب تكون التوصية هي السماح لحركة مرور البيانات إلى بوابة SSE استنادا إلى URL بدلا من عنواني IP.

في حالة عدم إنشاء هذا الاتصال، لا يتم إرسال الأحداث إلى بوابة SSE، وهذا مثال على اتصال ثابت بين FTD وبوابة SSE:

```
root@firepower:# lsof -i | grep conn
connector 13277   www   10u  IPv4 26077573      0t0  TCP localhost:8989 (LISTEN)
connector 13277   www   19u  IPv4 26077679      0t0  TCP 192.168.1.200:56495->ec2-35-172-147-
246.compute-1.amazonaws.com:https (ESTABLISHED)
```

المشكلات الشائعة

بعد الترقية إلى 6.4، لا يتصل موصل SSE بمدخل SSE. يوفر Connector.log أخطاء مماثلة للأحداث:(*Service).Start] تعذر الاتصال بنقطة نهاية ZeroMQ PUSH: تعذر الاتصال ب \"ipc:///ngfw/var/sf/run/EventHandler_SSEConnector.sock\": اطلب unix /ngfw/var/sf/run/EventHandler_SSEConnector.sock: الاتصال: لا يوجد مثل هذا الملف أو الدليل\n"

إعادة تشغيل خدمة SSEConnector:

1) تعطيل Sudo Pmtool SSEConnector

2) SUDO PMTOOL enableByid SSEConnector

3) قم بإعادة تشغيل الجهاز. عند إعادة التشغيل، يتصل الجهاز بالسحابة.

المواقع الهامة لملفات السجل

سجلات التصحيح - ظهر الاتصال الناجح أو رسائل الفشل

```
/ngfw/var/log/connector/connector.log
```

إعدادات التكوين

```
/ngfw/etc/sf/connector.properties
```

إعدادات التكوين

```
curl localhost:8989/v1/contexts/default
```

معلومات ذات صلة

- https://docs.castle.amp.cisco.com/CiscoSecurityAccountUserGuide.pdf
- الدعم التقني والمستندات - Cisco Systems

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).