المرحلة 3 من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها: ذكاء الأمان

المحتويات

المقدمة

هذه المقالة هي جزء من سلسلة مقالات توضح كيفية أستكشاف مسار البيانات في أنظمة FirePOWER وإصلاحها بشكل منهجي لتحديد ما إذا كانت مكونات FirePOWER قد تؤثر على حركة المرور. يرجى الرجوع إلى مقالة "نظرة عامة" للحصول على معلومات حول بنية الأنظمة الأساسية FirePOWER وارتباطاتها بمقالات "أستكشاف أخطاء مسارات البيانات وإصلاحها" الأخرى.

يغطي هذا المقال المرحلة الثالثة من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها، وهي ميزة "معلومات الأمان".

المتطلبات الأساسية

- يتعلق هذا المقال بجميع منصات FirePOWER المدعومة حاليا
- تم إدخال معلومات الأمان لعناوين URL و DNS في الإصدار 6.0.0

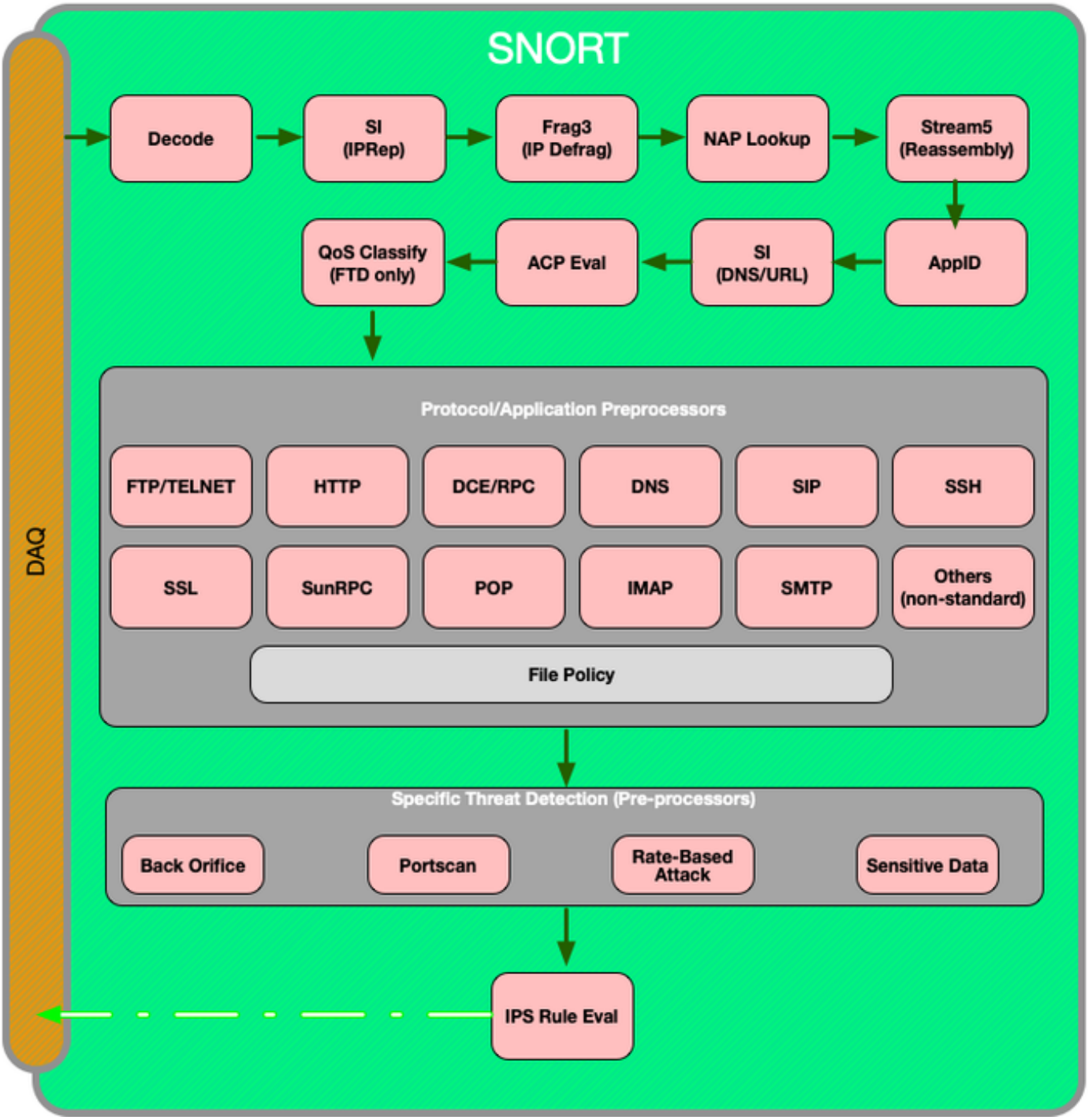
أستكشاف أخطاء مرحلة معلومات أمان FirePOWER وإصلاحها

تعتبر الاستخبارات الأمنية ميزة تقوم بعمليات تفتيش ضد القوائم السوداء والجهات البيضاء على حد سواء من أجل:

- عناوين IP (المعروفة أيضا باسم "الشبكات" في أجزاء معينة من واجهة المستخدم)
- محددات موقع الموارد الموحد (URLs)
- استعلامات نظام اسم المجال (DNS)

يمكن علم القوائم الموجودة ضمن "ذكاء الأمان" بواسطة موجز ويب تم توفيره من قبل Cisco و/أو قوائم وموجز ويب تم تكوينها من قبل المستخدم.

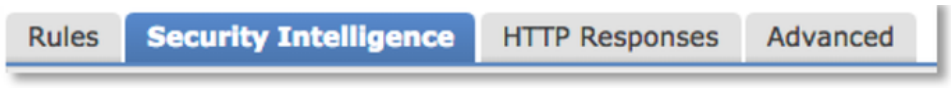
يعد "سمعة الذكاء الأمني" المستندة إلى عناوين IP المكون الأول داخل FirePOWER لفحص حركة المرور. يتم تنفيذ URL و DNS Security Intelligence بمجرد اكتشاف بروتوكول التطبيق ذي الصلة. فيما يلي رسم تخطيطي لسير عمل فحص برنامج Firepower.

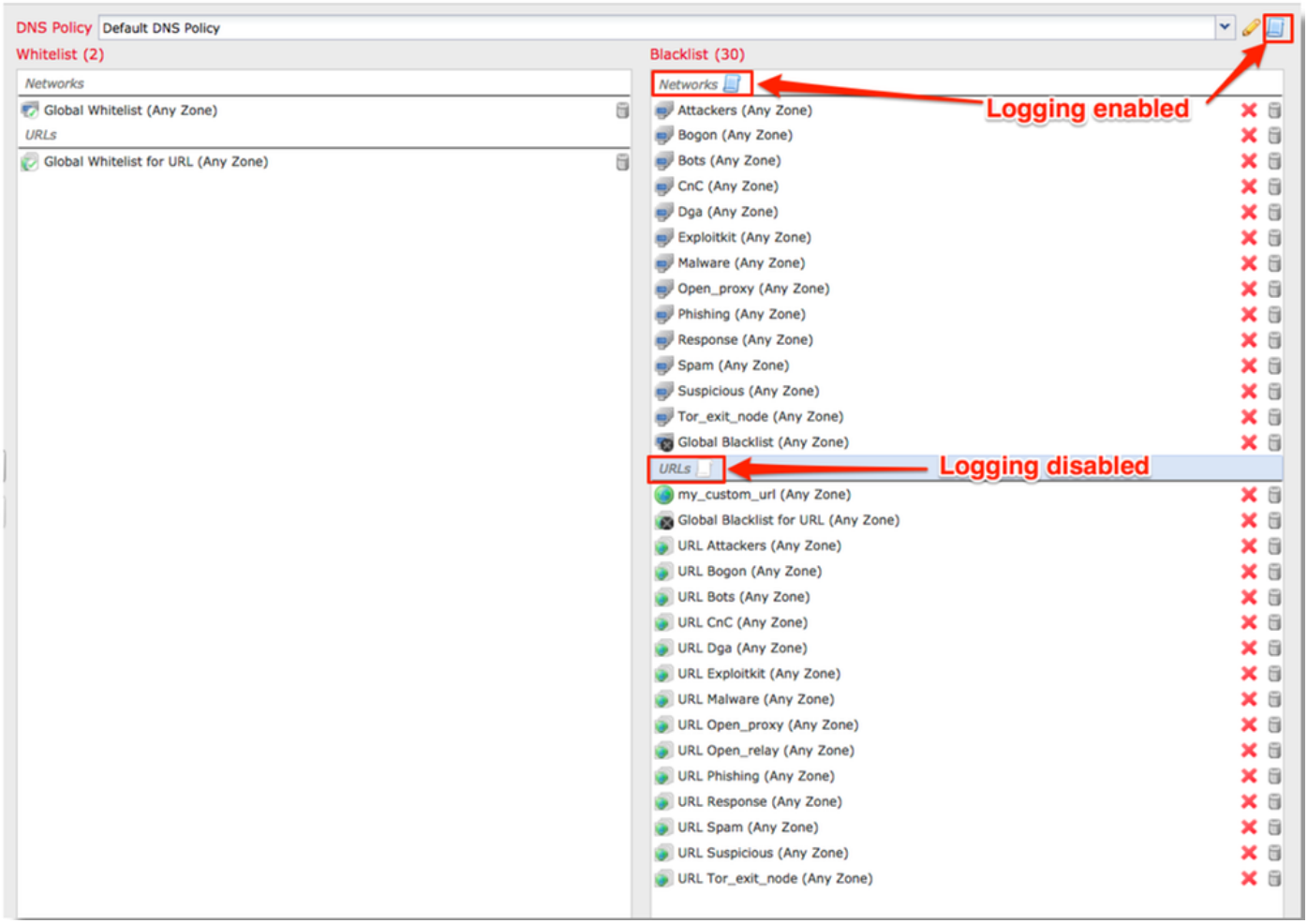


حدد تمكين التسجيل لأحداث الذكاء الأمني

يعد تحديد الكتل الموجودة على مستوى ذكاء الأمان سهلا للغاية طالما تم تمكين التسجيل. ويمكن تحديد ذلك على واجهة المستخدم (UI) لمركز إدارة Firepower (FMC) من خلال الانتقال إلى **السياسات > التحكم في الوصول > سياسة التحكم في الوصول**. بعد النقر

فوق رمز التحرير الموجود بجانب النهج قيد البحث، انتقل إلى علامة التبويب **معلومات الأمان**.



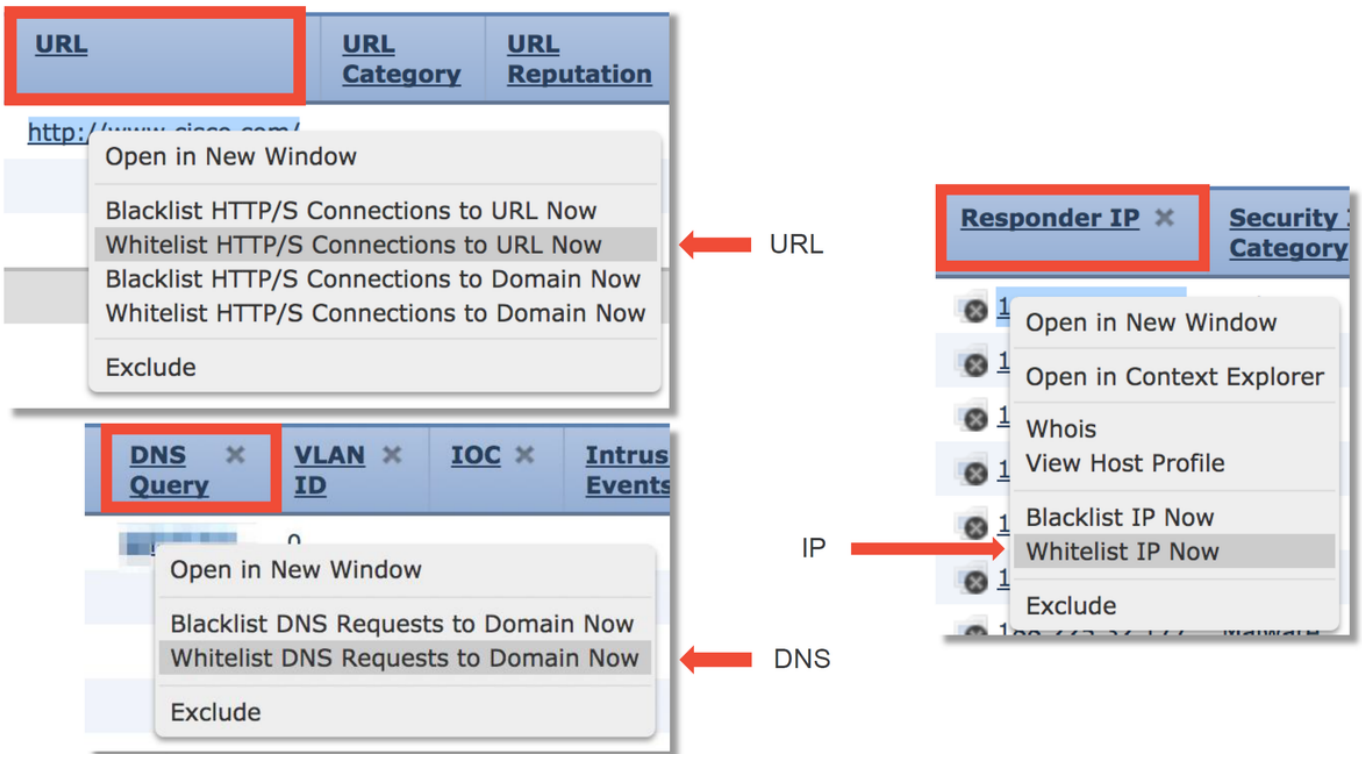


مراجعة أحداث الإستخبارات الأمنية

بمجرد تمكين التسجيل، يمكنك عرض أحداث ذكاء الأمان تحت **التحليل > الاتصالات > أحداث ذكاء الأمان**. يجب أن يكون واضحا سبب منع حركة المرور.

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Security Intelligence Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	192.168.1.95		DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95		Malware

كخطوة تخفيف سريعة، يمكنك النقر بزر الماوس الأيمن على IP أو URL أو استعلام DNS الذي يتم حظره بواسطة ميزة "معلومات الأمان" واختيار خيار البيانات البيضاء.



إذا كنت تشك في أن شيئا ما تم وضعه بشكل غير صحيح على القائمة السوداء، أو إذا كنت ترغب في طلب تغيير السمعة، يمكنك فتح تذكرة مباشرة مع Cisco Talos على الرابط التالي:

https://www.talosintelligence.com/reputation_center/support

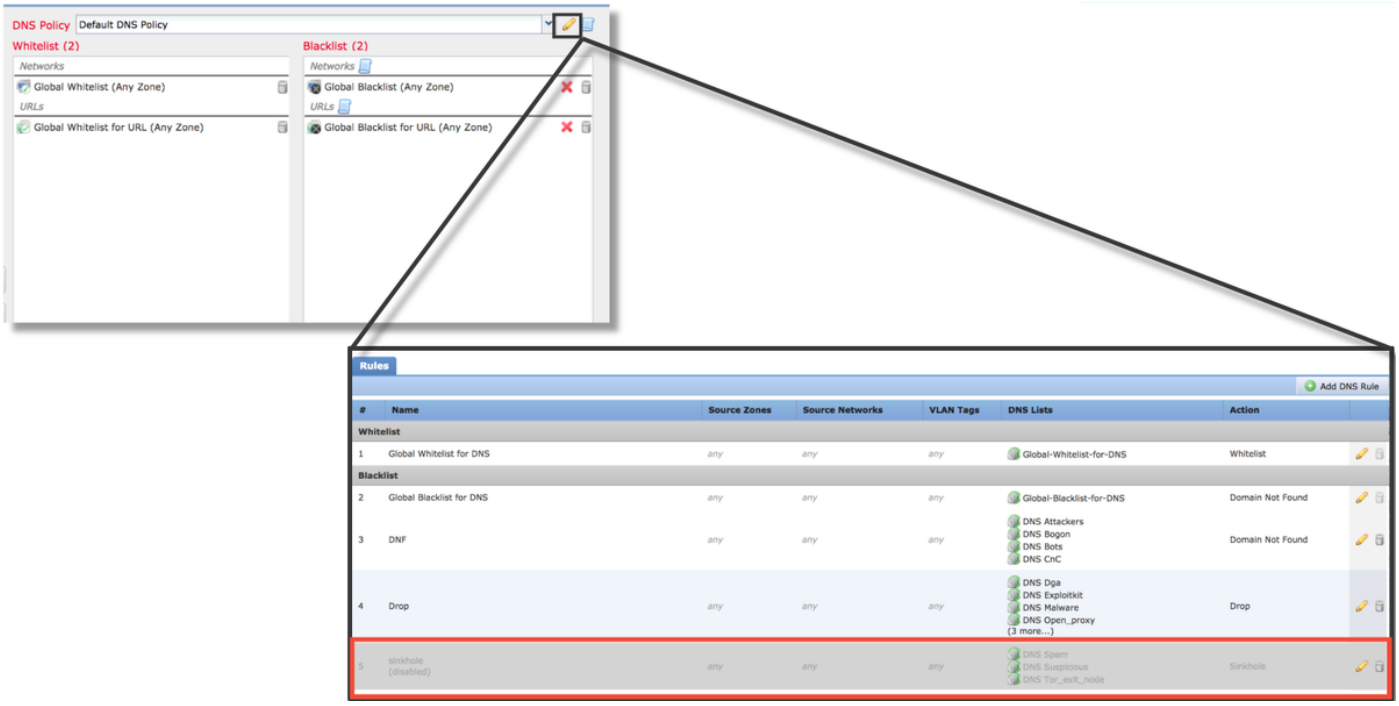
يمكنك أيضا توفير البيانات إلى مركز المساعدة التقنية (TAC) من Cisco للتحقيق في ما إذا كان يجب إزالة عنصر من القائمة السوداء.

> **ملاحظة:** إضافة عنصر إلى الشخص الأبيض يضيف إدخالا إلى المسؤول عن الاستخبارات الأمنية، مما يعني أنه سيمح لهذا الشيء بتمرير فحص إستخبارات الأمن. ومع ذلك، لا يزال بإمكان جميع مكونات Firepower الأخرى فحص حركة المرور.

كيفية إزالة تكوينات ذكاء الأمان

من أجل إزالة تكوينات ذكاء الأمان، انتقل إلى علامة التبويب **ذكاء الأمان**، كما هو مذكور أعلاه. هناك ثلاثة أقسام؛ واحد للشبكات، عنوان URL بالإضافة إلى سياسة DNS.

من هناك، يمكن إزالة القوائم ومووج الويب بالنقر على رمز trashcan.



لاحظ في لقطة الشاشة أعلاه، أنه قد تم إزالة جميع قوائم معلومات أمان IP و URL باستثناء القائمة السوداء العالمية والقائمة البيضاء.

ضمن نهج DNS، حيث يتم تخزين تكوين "معلومات أمان DNS"، يتم تعطيل إحدى القواعد.

> **ملاحظة**: لعرض محتويات القوائم السوداء العالمية والقوائم البيضاء، انتقل إلى **الكائنات > إدارة الكائنات > ذكاء الأمان**. ثم انقر فوق القسم محل الاهتمام (الشبكة، عنوان URL، DNS). سيؤدي تحرير القائمة بعد ذلك إلى عرض المحتويات، على الرغم من أنه يجب إجراء التكوين داخل نهج التحكم بالوصول.

التحقق من التكوين على الطرف الخلفي

يمكن التحقق من تكوين "ذكاء الأمان" على CLI عبر الأمر **> show access-control-config**، الذي يعرض محتويات نهج التحكم في الوصول النشط الجاري تشغيله على جهاز FirePOWER.

```
> show access-control-config

==================[ My AC Policy ]==================
Description             :
Default Action           : Allow
Default Policy           : SOC
Logging Configuration
   DC                  : Enabled
   Beginning           : Disabled
   End                 : Enabled
Rule Hits               : 0
Variable Set            : Default-Set

===[ Security Intelligence - Network Whitelist ]====
   Name                 : Global-Whitelist (List)
   IP Count             : 0
   Zone                 : any

===[ Security Intelligence - Network Blacklist ]====
Logging Configuration    : Enabled
   DC                  : Enabled


--------------------[ Block ]---------------------
   Name                 : Attackers (Feed)
   Zone                 : any

   Name                 : Bogon (Feed)
   Zone                 : any
...[omitted for brevity]
```

لاحظ في المثال أعلاه، أنه تم تكوين التسجيل للقائمة السوداء للشبكة وتم تضمين إثنين على الأقل من موجز الويب في القائمة السوداء (المهاجمين و Bogon).

يمكن تحديد ما إذا كان العنصر المفرد في قائمة ذكاء الأمان في وضع خبير. يرجى الاطلاع على الخطوات التالية:

```
> expert
$ grep <ip.addr> /var/sf/iprep_download/*
/var/sf/iprep_download/23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf:<ip.addr>

$ head -1 /var/sf/iprep_download/23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf
#Cisco intelligence feed: Malware



$ grep <url> /var/sf/siurl_download/*
/var/sf/siurl_download/00000000-0000-0ed3-0000-073014445223.lf:<url>

$ head -1 /var/sf/siurl_download/00000000-0000-0ed3-0000-073014445223.lf
#URL object: my_custom_url



$ grep <dns.hostname> /var/sf/sidns_download/*
/var/sf/sidns_download/032ba433-c295-11e4-a919-d4ae5275b77b.lf: <dns.hostname>

$ head -1 /var/sf/sidns_download/032ba433-c295-11e4-a919-d4ae5275b77b.lf
#Cisco DNS and URL intelligence feed: DNS Response
```

IP SI lists are in /var/sf/iprep_download/

URL SI lists are in /var/sf/siurl_download/

DNS SI lists are in /var/sf/sidns_download/

هناك ملف لكل قائمة معلومات الأمان الذكية مع UUID فريد. يوضح المثال أعلاه كيفية

تعريف اسم القائمة، باستخدام الأمر **head -n1**.

البيانات التي سيتم تقديمها إلى TAC

البيانات	تعليمات
أستكشاف أخطاء الملفات وإصلاحها من وحدة التحكم في إدارة الإطارات (FMC) وجهاز FirePOWER الذي يقوم بفحص حركة المرور لقطات شاشة للأحداث (مع تضمين الطوابع الزمنية)	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techn
مخرجات النص من جلسات عمل CLI في حالة إرسال حالة إيجابية خاطئة، قم بتوفير العنصر (IP، URL، المجال) للنزاع.	طالع هذه المقالة للحصول على تعليمات
	طالع هذه المقالة للحصول على تعليمات
	تقديم الاسباب والادلة التي من اجلها يجب إجراء النزاع.

الخطوة التالية

إذا تم تحديد أن مكون "معلومات أمنية" ليس هو سبب المشكلة، فإن الخطوة التالية ستكون أستكشاف أخطاء قواعد سياسة التحكم بالوصول وإصلاحها.

انقر هنا لمتابعة المقالة التالية.

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).