

ةياهنلا ةطقنل IOC حسم تايلمع ذي فنت FireAMP وأ ةياهنلا طاقنل AMP مادختساب

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[معلومات أساسية](#)

[ملفات توقيع IOC](#)

[تشغيل المسح الضوئي على ملف توقيع IOC](#)

[إنشاء ملف توقيع IOC](#)

[تحميل ملف توقيع IOC](#)

[بدء الفحص](#)

المقدمة

يصف هذا وثيقة كيف أن يخلق إشارة إلى التسوية (IOC) توقيع مبرد من خلال مدير تحرير IOC، كيف أن يرفع هو إلى ال Cisco FireAMP لوحة معلومات، وكيف أن يبدأ نقطة نهاية IOC مسح.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن يكون لديك على الأقل جيبابيت واحد من مساحة محرك الأقراص الحرة قبل أن تحاول تشغيل عمليات المسح الضوئي IOC لنقطة النهاية.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى ماسح IOC لنقطة النهاية، والذي يتوفر في إصدارات Cisco FireAMP Windows Connector 4.0.2 والإصدارات الأحدث.

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

معلومات أساسية

إن ميزة مسح IOC الضوئي لنقطة النهاية هي أداة قوية للاستجابة للحوادث يتم استخدامها من أجل مسح مؤشرات ما بعد التسوية عبر أجهزة كمبيوتر متعددة.

ملاحظة: على الرغم من أن FireAMP يدعم اللجنة الأوقيانوغرافية الحكومية الدولية بلغة الإدارة، إلا أن برنامج محرر اللجنة الأوقيانوغرافية الحكومية الدولية المسؤول نفسه لم يطرره أو يدعمه Cisco. لا يقوم دعم Cisco باكتشاف أخطاء IOCs التي أنشأها المستخدم أو التي قامت بإنشائها جهة خارجية وإصلاحها.

ملفات توقيع IOC

ملف توقيع IOC هو مخطط XML قابل للتوسيع لوصف الخصائص التقنية التي تحدد التهديد المعروف، منهجية المهاجم، أو دليل آخر على التسوية.

يمكنك إستيراد IOCs لنقطة النهاية من خلال وحدة التحكم من الملفات المستندة إلى OpenIOC والتي تتم كتابتها لتشغيل خصائص الملف مثل الاسم والحجم والتجزئة، بالإضافة إلى سمات أخرى وخصائص النظام مثل معلومات العملية والخدمات قيد التشغيل وإدخالات سجل Microsoft Windows. يمكن إستخدام اللجنة الأوقيانوغرافية الحكومية الدولية من قبل المستجيبين للحوادث من أجل العثور على قطع أثرية معينة أو من أجل إستخدام المنطق لإنشاء عمليات كشف معقدة ومترابطة لعائلات البرامج الضارة.

تشغيل المسح الضوئي على ملف توقيع IOC

هناك ثلاث خطوات يجب عليك إكمالها لتشغيل المسح الضوئي على ملف توقيع IOC:

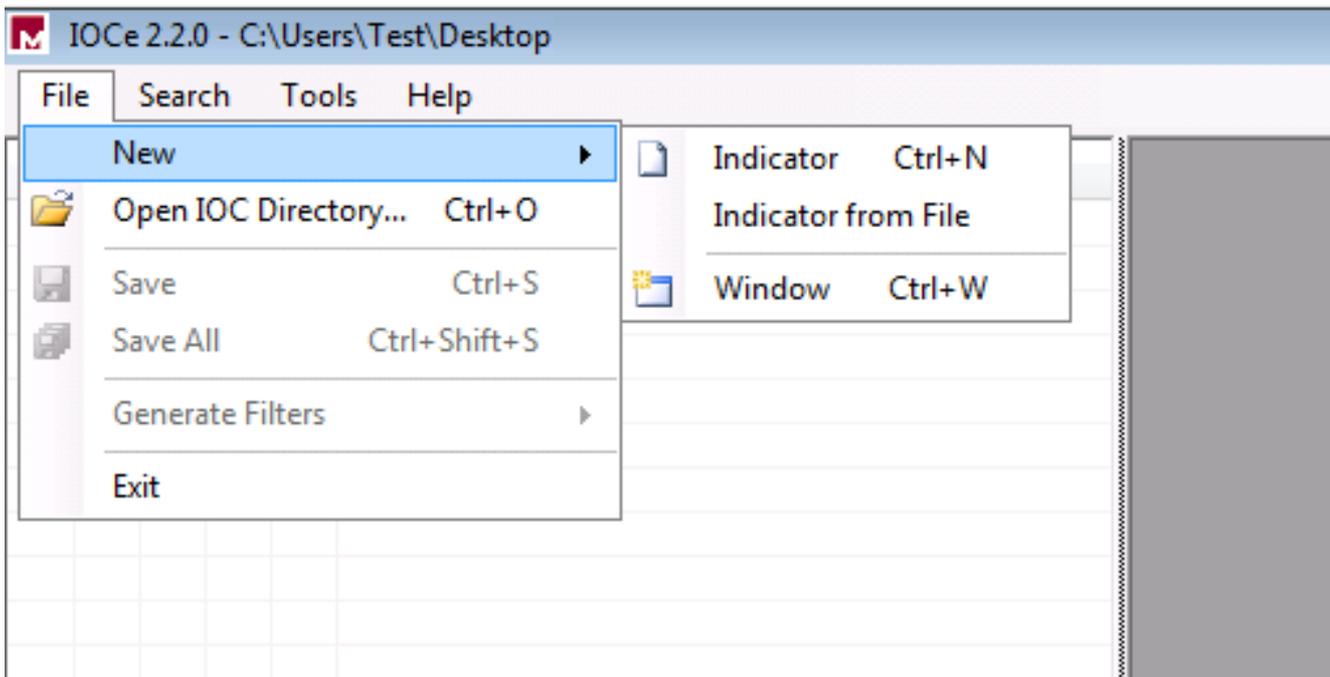
1. إنشاء ملف توقيع IOC.
 2. تحميل ملف توقيع IOC.
 3. ابدأ الفحص.
- ويجري توسيع نطاق هذه الخطوات في الأقسام التالية.

إنشاء ملف توقيع IOC

ملاحظة: في هذا المثال، يتم إستخدام محرر IOC المتنقل لإنشاء ملف توقيع IOC لملف نصي يسمى `test.txt`.

أكمل الخطوات التالية لإنشاء ملف توقيع IOC:

افتح IOCe وتصفح إلى ملف < جديد > مؤشر. يوفر ذلك مساحة عمل فارغة بحيث يمكنك البدء في بناء IOC.1.



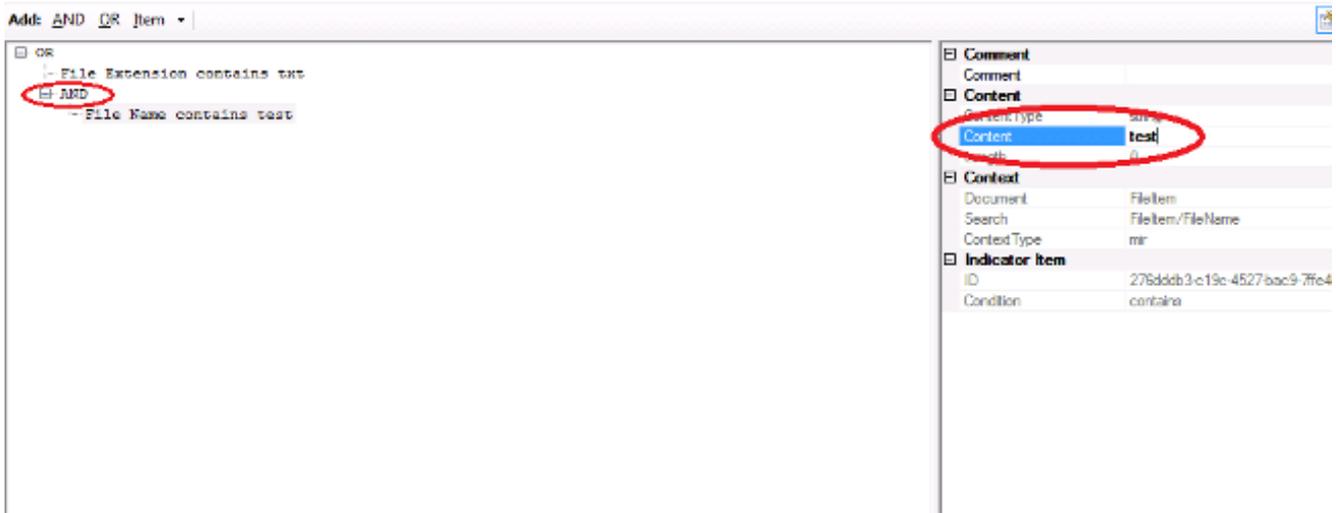
ملاحظة: من أجل إنشاء IOC لشيء محدد، أستخدم المنطق الثنائي مع الخصائص. المشغل الأولي هو OR، وهو أبسط قاعدة للعمل من. وهذا يسمح للوظيفة الأولية للجنة الأوقيانوغرافية الحكومية الدولية بالعمل، لذلك لا يطلب منك تغييرها. من المطلوب أن يحتوي ملف توقيع IOC على خصائص أو شروط على الأقل لاستخدامها بنجاح في المسح الضوئي.

2. انقر فوق القائمة المنسدلة العناصر لإضافة عوامل تشغيل. الخاصية الأولى التي يجب إضافتها هي **File Extension** (ملحق الملف). ابحث عن الخاصية في قائمة شجرة العناصر وانقر فوقها.

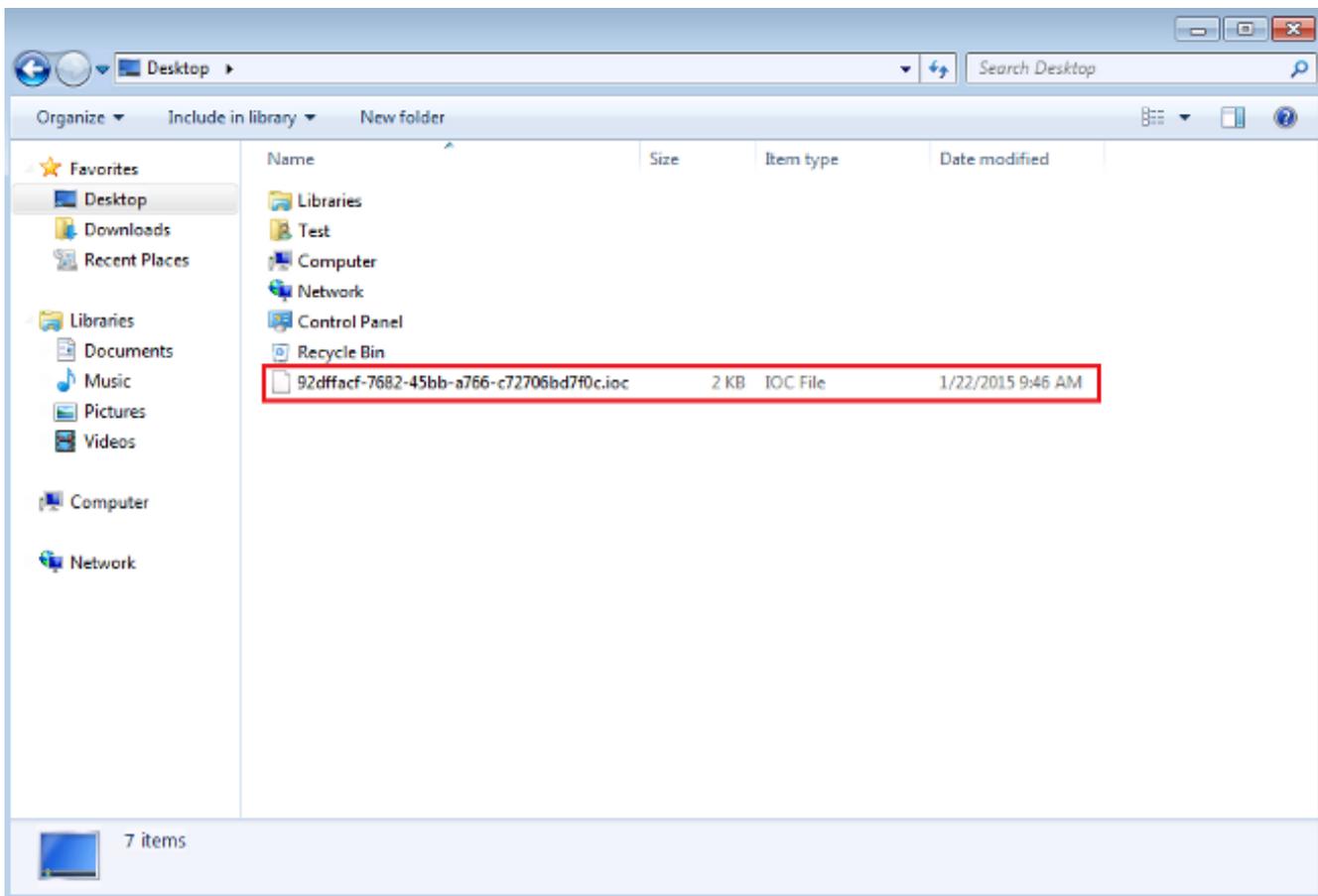
3. بعد إضافة خاصية، انقر فوق الأيقونة الصغيرة الموجودة في أقصى الجانب الأيمن من الشاشة لفتح جزء التكوين. ضمن هذا الجزء، أستخدم حقل المحتوى لمطابقة ملحق ملف. على سبيل المثال، أضف **txt** لمطابقة الملف النصي **test.txt**:



4. يجب أن تقوم الآن بإضافة عامل تشغيل منطق. في هذا المثال، ستطابق ملف إختبار النص. ولمطابقة هذا الأمر، أستخدم مشغل AND وأضف الخاصية التالية. حدد مكان اسم الملف وحدده من قائمة شجرة العناصر. في جزء "الخصائص"، قم بإضافة اسم الملف الذي تريد البحث عنه. على سبيل المثال، أضف إختبار في حقل المحتوى:



5. بما أنه لا توجد خصائص إضافية لازمة للجنة الأوقيانوغرافية الحكومية الدولية البسيطة، يمكنك الآن حفظ الملف. انقر فوق ملف < حفظ، ويتم حفظ ملف توقيع بملحق IOC على النظام:



تحميل ملف توقيع IOC

لإجراء مسح ضوئي، يجب تحميل ملف IOC إلى لوحة معلومات FireAMP. يمكنك استخدام ملف توقيع IOC، ملف XML، أو أرشيف ZIP يحتوي على ملفات IOC متعددة. تقوم لوحة المعلومات بإلغاء ضغط الملف وتحليله باستخدام توقعات IOC. يتم إخطارك في حالة استخدام بناء جملة غير صحيح أو خاصية غير مدعومة.

تلميح: يمكنك تحميل الملفات التي يصل حجمها إلى 5 ميغابايت.

أكمل الخطوات التالية لتحميل ملف توقيع IOC إلى لوحة معلومات FireAMP:

قم بتسجيل الدخول إلى وحدة تحكم سحابة FireAMP وانتقل إلى التحكم في التفشي < نقطة النهاية المثبتة>.IOC

2. انقر تحميل، وتظهر نافذة تحميل نقطة النهاية IOCs:

Upload Endpoint IOCs ×

You can upload a single Endpoint IOC XML file, or a .zip file containing multiple Endpoint IOC documents

There is a 5 megabyte file upload limit

No file selected

بعد تحميل ملف توقيع IOC بنجاح، يظهر التوقيع على القائمة:

Endpoint IOC - Installed Endpoint IOCs ^{beta}

Categories Groups Keywords

Showing

<input type="checkbox"/> Test 59c4cc2d-e1e7-489f-93fd-30596fda0052.ioc	Uploaded: 9:20 AM Eastern Standard Time, 1/22/2015	Active	<input type="button" value="View"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Refresh"/>
---------------------------------------------------------------------------	-------------------------------------------------------	--------	-------------------------------------	-------------------------------------	---------------------------------------	----------------------------------------

3. انقر فوق عرض لعرض بيانات XML الفعلية للتوقيع:

Endpoint IOC beta

File name: 59c4cc2d-e1e7-489f-93fd-30596fda0052.ioc

View All

View

Edit

Active

Short Description:

Test

Description

No description given

Categories

No Categories to display

IOC Groups

No IOC Groups to display

Keywords

No Keywords to display

Source [Download]

```
1 <?xml version="1.0" encoding="us-ascii"?>
2 <ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
3 id="59c4cc2d-e1e7-489f-93fd-30596fda0052" last-modified="2015-01-22T14:18:48" xmlns="http://schemas.mandiant.co
4 /2010/ioc">
5   <short_description>Test</short_description>
6   <authored_by>Test Author</authored_by>
7   <authored_date>2015-01-22T14:16:39</authored_date>
8   <links />
9   <definition>
10     <Indicator operator="OR" id="325adecc-d75e-4fae-9cf4-cf8dcae84a36">
11       <IndicatorItem id="5311e18c-0e6a-4491-bba1-a63331a463a2" condition="contains">
12         <Context document="FileItem" search="FileItem/FileExtension" type="mir" />
13         <Content type="string">txt</Content>
14       </IndicatorItem>
15       <IndicatorItem id="017fc010-f0ea-4ede-b252-885bb85cfcf3">
16         <IndicatorItem id="6ac73c61-9e9f-43da-9317-38d09990c337" condition="contains">
17           <Context document="FileItem" search="FileItem/FileName" type="mir" />
18           <Content type="string">test</Content>
19         </IndicatorItem>
20       </IndicatorItem>
21     </Indicator>
22   </definition>
23 </ioc>
```

بدء الفحص

بعد تحميل ملف توقيع، قم بإجراء فحص كامل. يجب أن يكون الفحص الأول مسحاً ضوئياً كاملاً لأنه يجب أن يقوم بإنشاء كتالوج بيانات تعريف للكمبيوتر بأكمله، والذي قد يستغرق من ساعة إلى ساعتين. يمكنك إجراء مسح فلاش بعد فهرسة النظام من خلال مسح كامل.

ملاحظة: يعد الفحص الكامل مكثفاً جداً لوحدة المعالجة المركزية. توصي Cisco بعدم تشغيل فحص كامل على جهاز كمبيوتر أثناء استخدامه. إذا كنت تخطط لاستخدام الميزة بشكل منتظم، فيمكنك إجراء فحص كامل مرة في الشهر لإعادة إنشاء الكتالوج.

هناك طريقتان مختلفتان يمكنك استخدامهما لتشغيل مسح IOC. تتمثل الطريقة الأولى في إجراء فحص فوري للحدث أو من لوحة المعلومات. يتم تشغيل هذا في المرة التالية التي يرسل فيها جهاز كمبيوتر نبضات القلب إلى السحابة.

ملاحظة: إذا كانت هذه هي المرة الأولى التي تقوم فيها بتشغيل الفحص الكامل، فلن يطلب منك التحقق من إعادة الكتالوج قبل خيار المسح الضوئي.

Run Scan on win7



Windows 7, SP 1.0 Device in
IOC Test using IOC Test

Scan Engine:

File

Endpoint IOC

Scan Depth:

Flash

Full

1 Endpoint IOC active.

Re-catalog before scan

Running a full scan is **time consuming and resource intensive**. On endpoints with a large number of files a full scan can take multiple days to run. You should only run a full scan during non-business hours otherwise consider running a flash scan.

Close

Start Scan

الطريقة الثانية هي إنشاء نقطة نهاية مجدولة مسح IOC من قائمة التحكم في التفشي الخاصة بلوحة المعلومات. قد يكون هذا الخيار مثاليا عندما ترغب في إجراء عمليات مسح ضوئي أثناء ساعات غير الذروة. يجب توفير بيانات اعتماد حساب لديه إذن على الكمبيوتر المحدد لإنشاء مهام مجدولة والسماح بتسجيل الدخول ك إذن نهج مجموعة دفعات.

Endpoint IOC - Initiate Scan ^{beta}

Policy:

IOC Test

Scheduled Scan User Name:

Test

Scheduled Scan Password:

••••••••

Run Scan On:

2015-01-22

09

:

30

Flash scan

Full scan

Re-catalog before scan

Schedule Scan

1 Active Endpoint IOC

1 group using IOC Test with 1 Endpoint IOC capable connector out of 1 total connector

- loc test with 1 Endpoint IOC capable connector out of 1 total connector

عندما تقوم بجدولة نقطة نهاية مسح IOC، تظهر رسالة التحذير هذه:

Warning



Running a full scan is **time consuming** and **resource intensive**. On endpoints with a large number of files a full scan can take multiple days to run. You should only run a full scan during non-business hours otherwise consider running a flash scan.

You have selected to re-catalog before a full scan, which can take longer to complete. You may not need to re-catalog if you recently ran a full scan with re-catalog.

Are you sure you want to schedule a full scan ?

Close

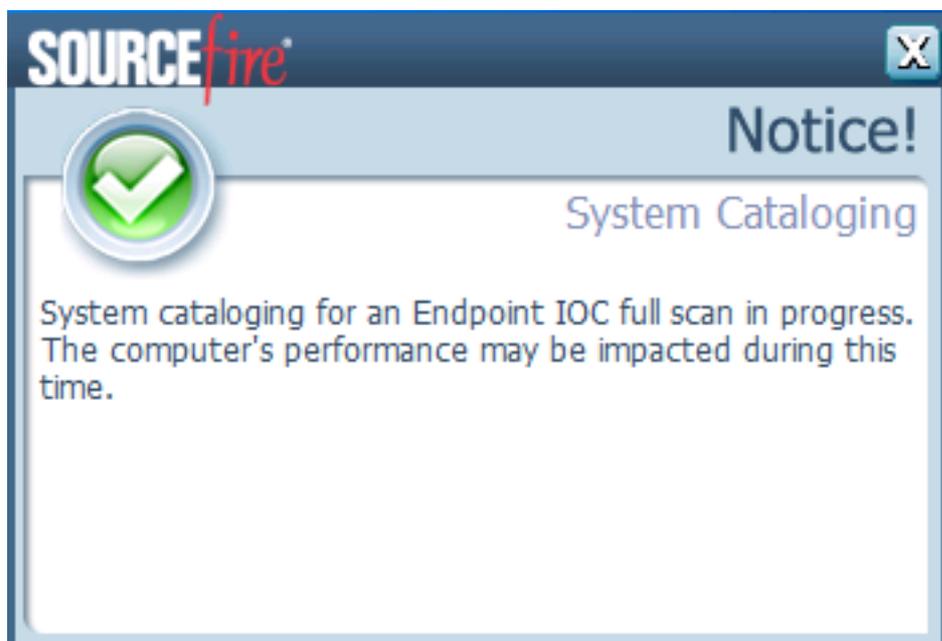
Schedule

في المرة التالية التي يرسل فيها جهاز الكمبيوتر الخاص بك ضربات القلب، وإذا كانت بيانات اعتمادك صالحة، فيجب أن ترى مهمة مماثلة لهذه في "مجدول مهام Windows":

Name	Status	Triggers	Next Run Time
Immunet Scan 1421937278	Ready	At 9:40 AM on 1/22/2015	1/22/2015 9:40:00 AM

عندما يبدأ الفحص، تظهر هذه الرسالة:

ملاحظة: إذا تم تكوين واجهة المستخدم الرسومية (GUI) لتكون مخفية، فلن ترى إشعار فهرسة النظام.



عند اكتمال المسح، يمكنك عرض ملخص اكتشاف المسح الضوئي لـ *Endpoint IOC*. يوضح هذا المثال تطابقا لملف توقع IOC **Test.txt**:

Win7 Scanned 16713078 objects. Found 655 matching objects and 0 malicious detections. Endpoint IOC Scan with Detections 11:55 AM Eastern Standard Time, 1/22/2015

Connector Info	Computer:	win7
Comments	Connector GUID:	a0881bab-af05-402c-e7c8-0bf0824a6638
	Current User:	

Run Scan Launch Device Trajectory

Win7 Endpoint IOC Scan Detection Summary (matched 1 of 1 IOCs) Endpoint IOC Scan Detection Summary 11:55 AM Eastern Standard Time, 1/22/2015

Endpoint IOC Summary	Matching Endpoint IOCs:	Test [Filename: 59c4cc2d-e1e7-489f-93fd-305968da0052.ioc]
Connector Info		
Comments		

View All

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء ف ن مء دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوءو تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل