

使用面向終端的AMP或FireAMP執行終端IOC掃描

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[IOC簽名檔案](#)

[對IOC簽名檔案運行掃描](#)

[建立IOC簽名檔案](#)

[上傳IOC簽名檔案](#)

[啟動掃描](#)

簡介

本文檔介紹如何通過Mandiant IOC編輯器建立危害表現(IOC)簽名檔案，如何將其上傳到Cisco FireAMP儀表板，以及如何啟動終端IOC掃描。

必要條件

需求

思科建議您在嘗試運行終端IOC掃描之前，至少擁有1 GB的可用驅動器空間。

採用元件

本文檔中的資訊基於終端IOC掃描程式，該掃描程式在Cisco FireAMP Windows聯結器4.0.2版及更高版本中可用。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

終端IOC掃描程式功能是一個強大的事件響應工具，用於掃描多台電腦上的危害後指示器。

附註：儘管FireAMP使用Mandiant語言支援IOC，但Mandiant IOC Editor軟體本身並未由思科開發或支援。思科支援不排除使用者建立或第三方IOC的故障。

IOC簽名檔案

IOC簽名檔案是一個可擴展的XML架構，用於描述識別已知威脅、攻擊者方法或其他危害證據的技術特徵。

您可以通過控制檯從基於OpenIOC的檔案匯入終端IOC，這些檔案被寫入以觸發檔案屬性（如名稱、大小和雜湊）以及其他屬性和系統屬性（如進程資訊、運行服務和Microsoft Windows登錄檔項）。突發事件響應者可使用IOC語法查詢特定對象，或使用邏輯為惡意軟體系列建立複雜的相關檢測。

對IOC簽名檔案運行掃描

要對IOC簽名檔案運行掃描，必須完成三個步驟：

1. 建立IOC簽名檔案。
2. 上傳IOC簽名檔案。
3. 啟動掃描。

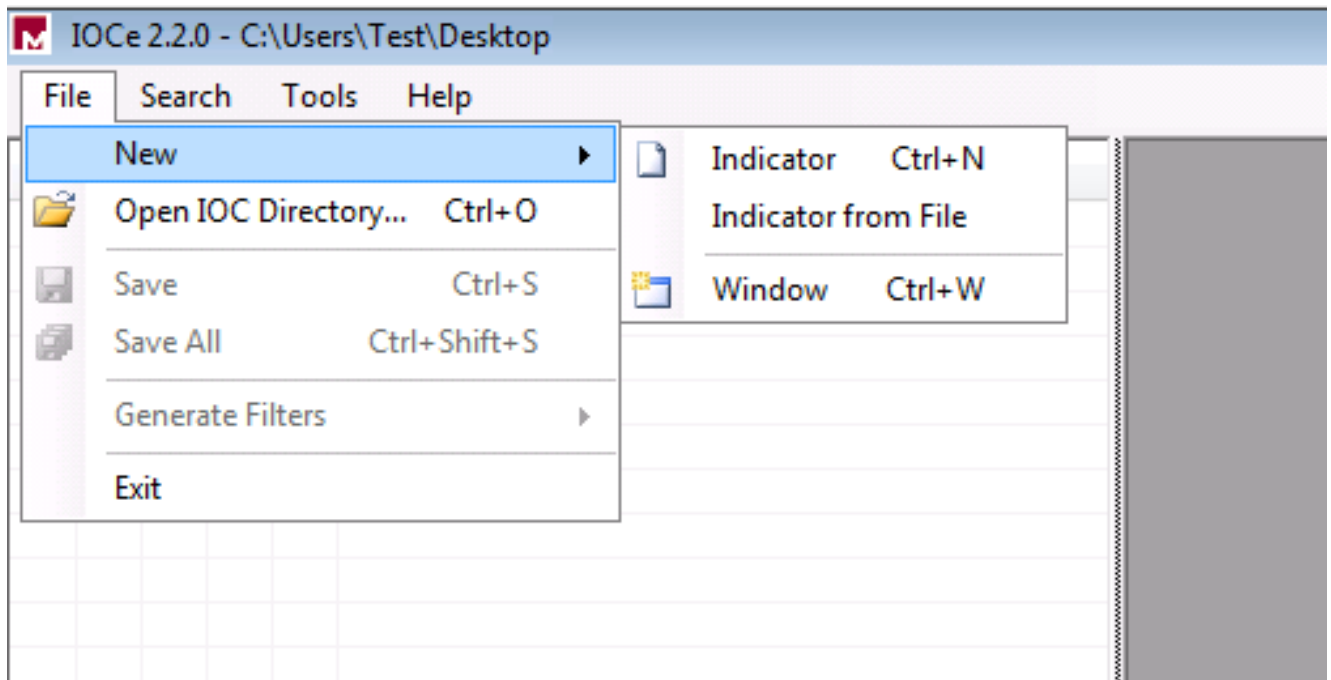
這些步驟將在後續章節中詳細介紹。

建立IOC簽名檔案

附註：在本示例中，使用Mandiant IOC編輯器為名為test.txt的文本檔案構建IOC簽名檔案。

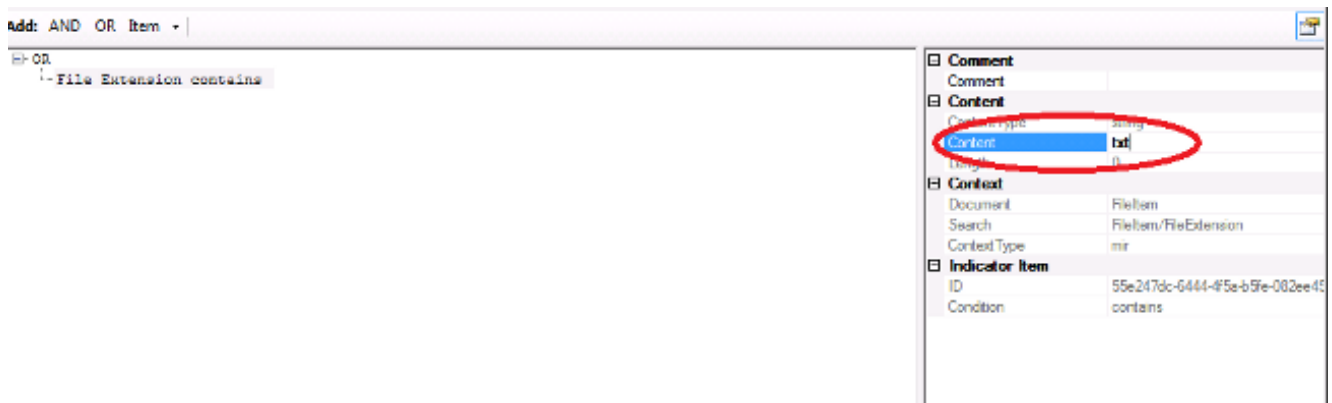
完成以下步驟以建立IOC簽名檔案：

1. 開啟IOCe並導航到**File > New > Indicator**。這將提供一個空白的工作區，以便您可以開始構建IOC。

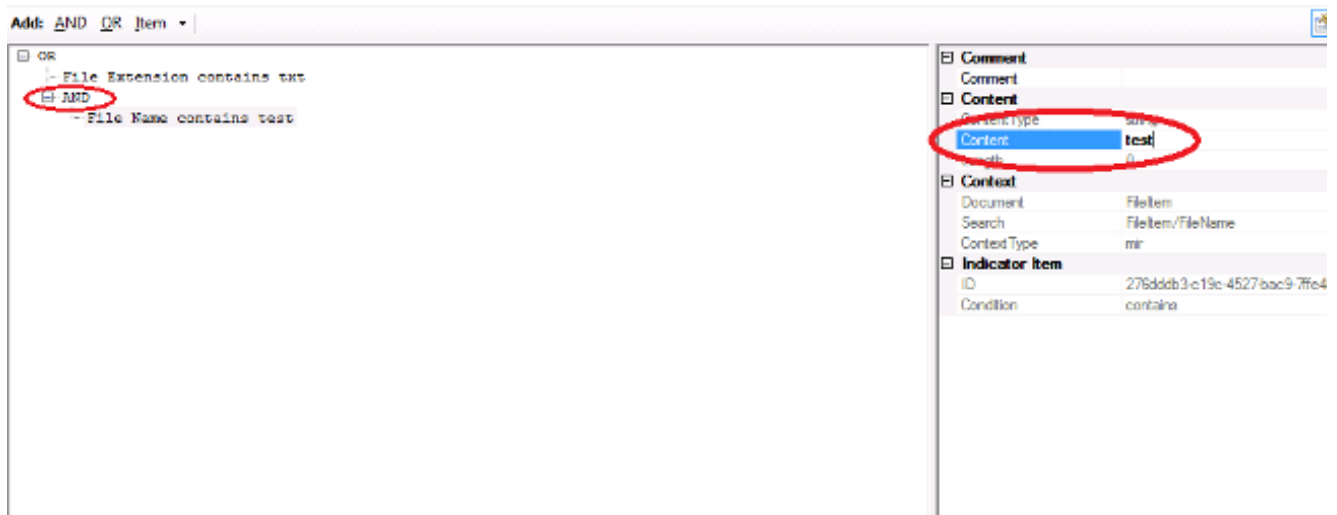


附註：要為特定對象建立IOC，請使用具有屬性的二進位制邏輯。初始運算子是OR，它是最簡單的基函式。這允許IOC的初始功能正常工作，因此您不需要更改它。要求IOC簽名檔案至少有兩個屬性或條件，才能在掃描中成功使用它。

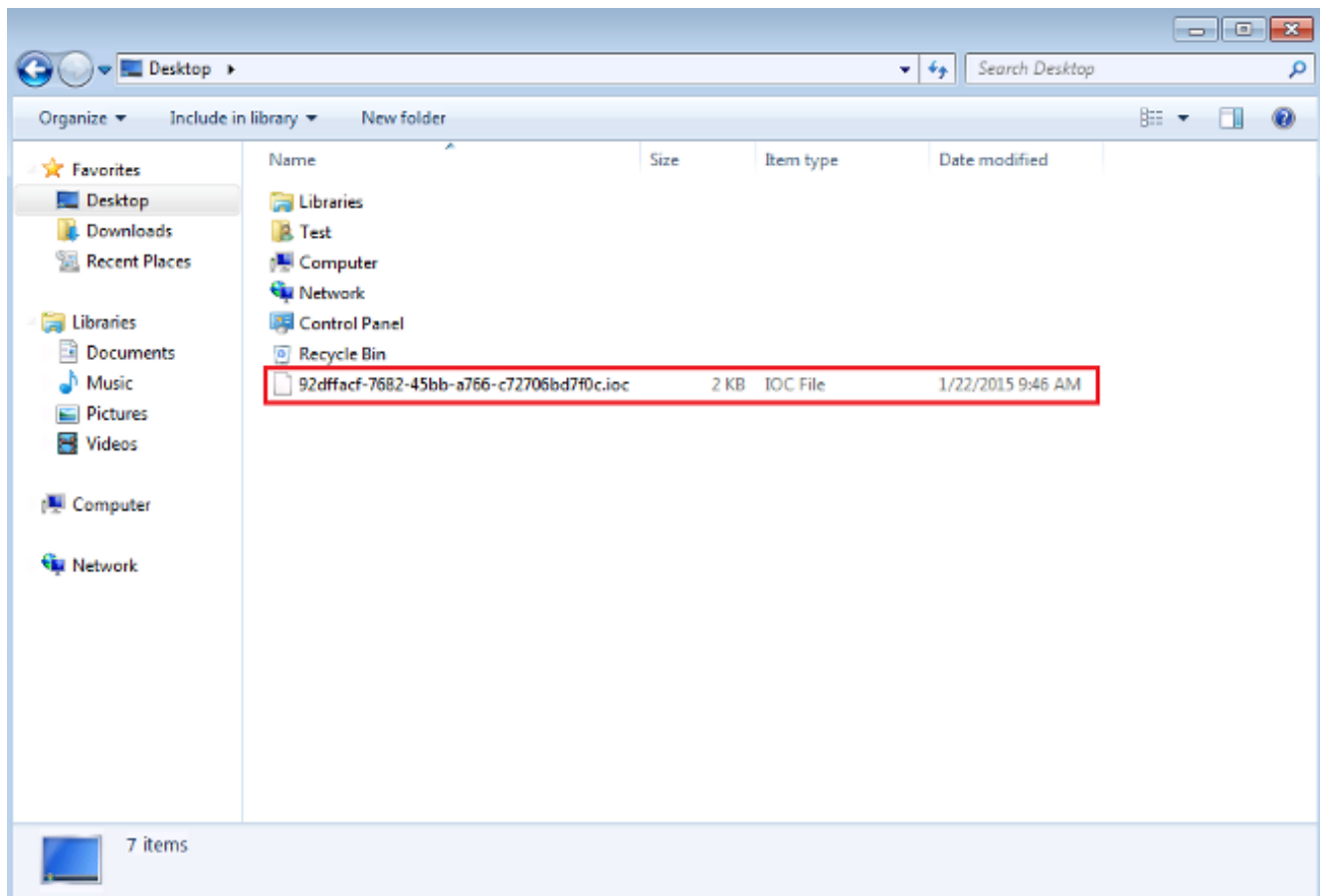
2. 按一下**Items**下拉選單以新增運算子。應新增的第一個屬性是**File Extension contains**。在「專案」樹選單中查找該屬性，然後按一下它。
3. 新增屬性後，按一下螢幕最右邊的小圖示以開啟「配置」窗格。在此窗格中，使用**Content**欄位以匹配副檔名。例如，新增**txt**以匹配**test.txt**文本檔案：



4. 現在必須新增邏輯運算子。在本示例中，您將匹配**測試**文本檔案。若要匹配該屬性，請使用**AND**運算子並新增下一個屬性。找到檔名，然後從「專案」(**Items**)樹選單中選擇。在「屬性」窗格中，新增要查詢的檔案的名稱。例如，在**Content**欄位中新增**test**:



5. 由於此簡單的IOC不需要其他屬性，現在您可以儲存檔案。按一下**File > Save**，此時系統上將儲存一個副檔名為*.ioc*的簽名檔案：



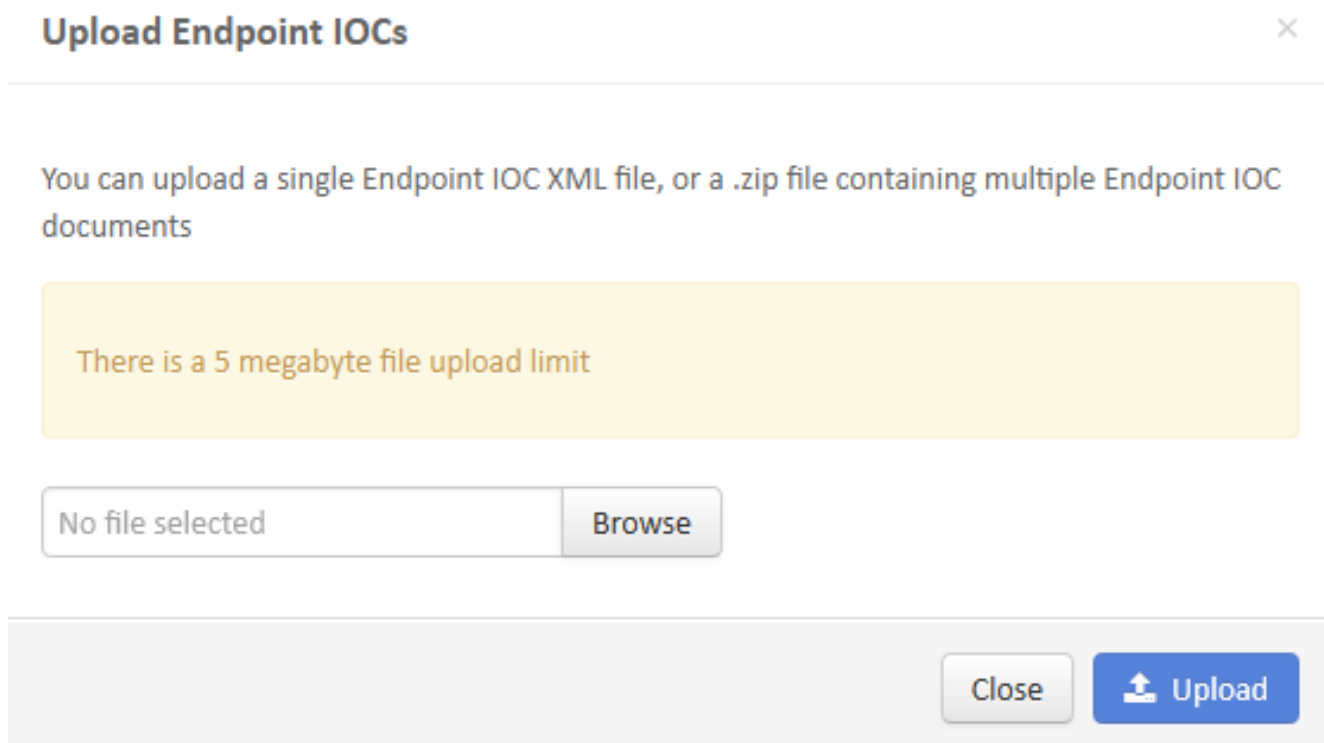
上傳IOC簽名檔案

為了執行掃描，您必須將IOC檔案上傳到FireAMP儀表板。您可以使用IOC簽名檔案、XML檔案或包含多個IOC檔案的zip存檔。儀表板使用IOC簽名解壓縮和解析檔案。如果使用不正確的語法或不支援的屬性，您將收到通知。

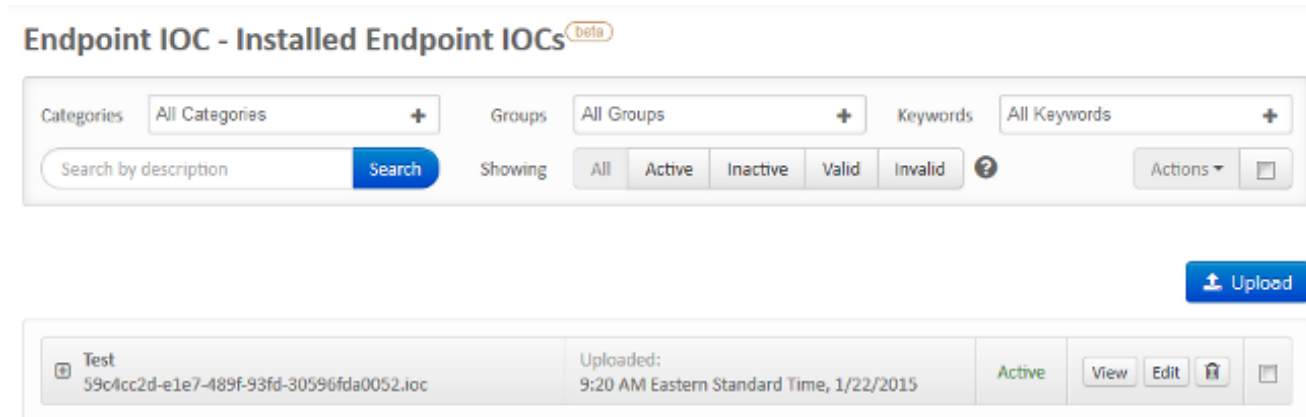
提示：您可以上傳大小最高為五百萬位元組的檔案。

完成以下步驟，以便將IOC簽名檔案上傳到FireAMP控制面板：

1. 登入到FireAMP雲控制檯，然後導航到Outbreak Control > Installed Endpoint IOC。
2. 點選Upload，此時會顯示Upload Endpoint IOCs視窗：



成功上載IOC簽名檔案後，該簽名將顯示在清單中：



3. 按一下檢視以檢視簽名的實際XML資料：

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>2015-01-22T14:16:35</authored_date>
8   <links />
9   <definition>
10    <Indicator operator="OR" id="325adeacd-d75e-4fae-9cf4-cf8dcae84a36">
11      <IndicatorItem id="5311e18c-0e6a-4491-bb1a-a63331a463a2" condition="contains">
12        <Context document="FileItem" search="FileItem/FileExtension" type="mir" />
13        <Content type="string">txt</Content>
14      </IndicatorItem>
15      <Indicator operator="AND" 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      </Indicator>
21    </Indicator>
22  </definition>
23 </ioc>
```

啟動掃描

上傳簽名檔案後，執行完全掃描。第一次掃描必須是完全掃描，因為它必須為整個電腦構建一個後設資料目錄，這可能需要1-2個小時。您可以通過完全掃描對系統編錄後，執行flash掃描。

附註：完全掃描佔用大量CPU。思科建議您不要在PC正在使用時對其進行完全掃描。如果您計畫定期使用該功能，則可以每月執行一次完全掃描以重建目錄。

運行IOC掃描可以使用兩種不同的方法。第一種方法是從事件或儀表板執行立即掃描。下次PC向雲傳送心跳時觸發此功能。

附註：如果這是第一次運行完全掃描，則不需要選中Re-catalog before scan選項。

Run Scan on win7



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

1 Endpoint IOC active.

Scan Engine:

File

Endpoint IOC

Scan Depth:

Flash

Full

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

第二種方法是從儀表板的**爆發控制**選單建立計畫的終端IOC掃描。當您希望在非高峰時間執行掃描時，此選項可能非常理想。必須提供擁有給定電腦許可權的帳戶的憑據，才能建立計畫任務並允許以**Batch組策略**身份登入許可權。

Endpoint IOC - Initiate Scan ^{beta}

Policy:

Scheduled Scan User Name:

Scheduled Scan Password:

Run Scan On: :

Flash scan Full scan

Re-catalog before scan

1 Active Endpoint IOC

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

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

計畫終端IOC掃描時，將顯示以下警告消息：

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

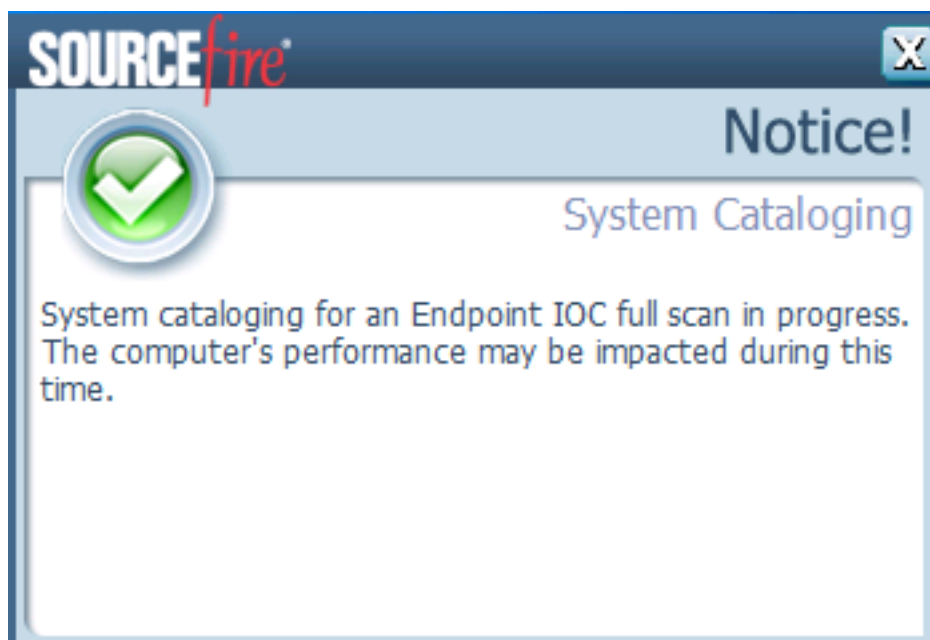
Schedule

下次您的PC傳送心跳時，如果您的憑據有效，您應該在Windows任務計畫程式中看到類似以下內容的作業：

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

掃描開始時，會出現以下消息：

附註：如果將GUI配置為隱藏，則看不到系統編目通知資訊。



掃描完成後，您可以檢視終端IOC掃描檢測摘要。此示例顯示test.txt IOC簽名檔案的匹配項：

The screenshot displays two panels from a security dashboard. The top panel, titled "Win7 Scanned 16713078 objects. Found 655 matching objects and 0 malicious detections", shows details for a scan on a computer named "win7". It lists the Connector GUID as "a068bbab-af05-402c-a7c8-6bf0824a6638" and the Current User as blank. A "Run Scan" button is visible. The bottom panel, titled "Win7 Endpoint IOC Scan Detection Summary (matched 1 of 1 IOCs)", shows a single matching IOC: "Test [Filename: 59c4cc28-e1e7-489f-93fd-305968da0052.txt]". A "View All" button is present below the list.

Panel	Title	Content
Win7	Scanned 16713078 objects. Found 655 matching objects and 0 malicious detections	Computer: win7 Connector GUID: a068bbab-af05-402c-a7c8-6bf0824a6638 Current User: Run Scan
Win7	Endpoint IOC Scan Detection Summary (matched 1 of 1 IOCs)	Matching Endpoint IOCs: Test [Filename: 59c4cc28-e1e7-489f-93fd-305968da0052.txt] View All