

# Esecuzione di analisi IOC degli endpoint con AMP for Endpoints o FireAMP

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[File di firma IOC](#)

[Eeguire un'analisi di un file di firma IOC](#)

[Creare un file di firma IOC](#)

[Carica un file di firma IOC](#)

[Avvia analisi](#)

## Introduzione

Questo documento descrive come creare un file di firma Indication of Compromise (IOC) tramite l'editor IOC Mandiant, come caricarlo sul dashboard Cisco FireAMP e come avviare una scansione IOC dell'endpoint.

## Prerequisiti

### Requisiti

Cisco consiglia di disporre di almeno un gigabyte di spazio libero sull'unità prima di tentare di eseguire le analisi IOC dell'endpoint.

### Componenti usati

Le informazioni di questo documento si basano sullo scanner IOC per endpoint, disponibile su Cisco FireAMP Windows Connector versione 4.0.2 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Premesse

La funzionalità dello scanner IOC dell'endpoint è un potente strumento di risposta agli incidenti utilizzato per eseguire la scansione degli indicatori post-compromissione in più computer.

**Nota:** Sebbene FireAMP supporti i CIO con il linguaggio Mandiant, il software Mandiant IOC Editor non è sviluppato né supportato da Cisco. Il supporto Cisco non esegue la risoluzione dei problemi dei COI creati dall'utente o di terze parti.

## File di firma IOC

Il file di firma IOC è uno schema XML estensibile per la descrizione delle caratteristiche tecniche che identificano una minaccia nota, una metodologia di attacco o altre prove di compromissione.

È possibile importare gli IOC degli endpoint tramite la console da file basati su OpenIOC scritti in modo da attivare proprietà dei file quali nome, dimensioni e hash, nonché altri attributi e proprietà di sistema quali informazioni sui processi, servizi in esecuzione e voci del Registro di sistema di Microsoft Windows. La sintassi IOC può essere utilizzata dai risponditori di incidenti per trovare artefatti specifici o per usare la logica per creare sofisticati rilevamenti correlati per famiglie di malware.

## Eseguire un'analisi di un file di firma IOC

Per eseguire un'analisi su un file di firma IOC, è necessario eseguire tre passaggi:

1. Creare un file di firma IOC.
2. Caricare il file della firma IOC.
3. Avviare un'analisi.

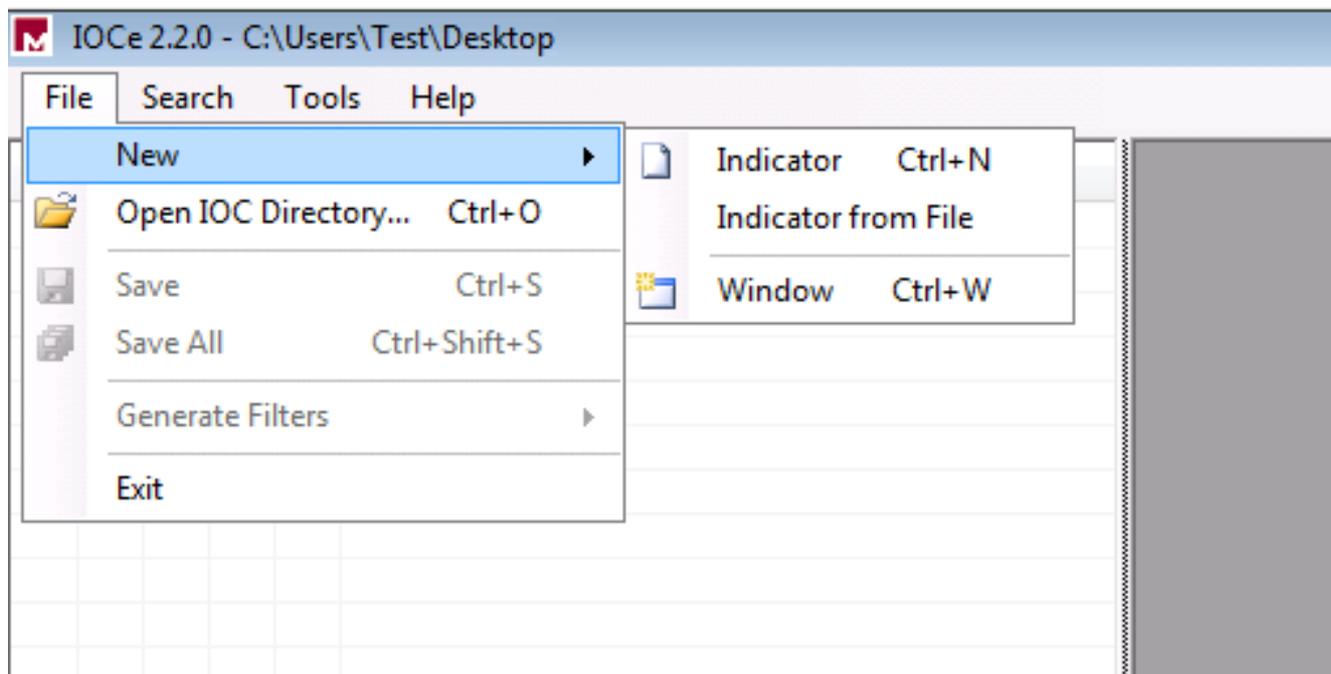
Nelle sezioni seguenti vengono illustrati i passaggi di questa procedura.

### Creare un file di firma IOC

**Nota:** In questo esempio, viene utilizzato l'editor IOC di Mandiant per creare un file di firma IOC per un file di testo denominato **test.txt**.

Completare questi passaggi per creare un file di firma IOC:

1. Aprire **IOCe** e selezionare **File > Nuovo > Indicatore**. In questo modo viene fornita un'area di lavoro vuota che consente di iniziare a creare un IOC.

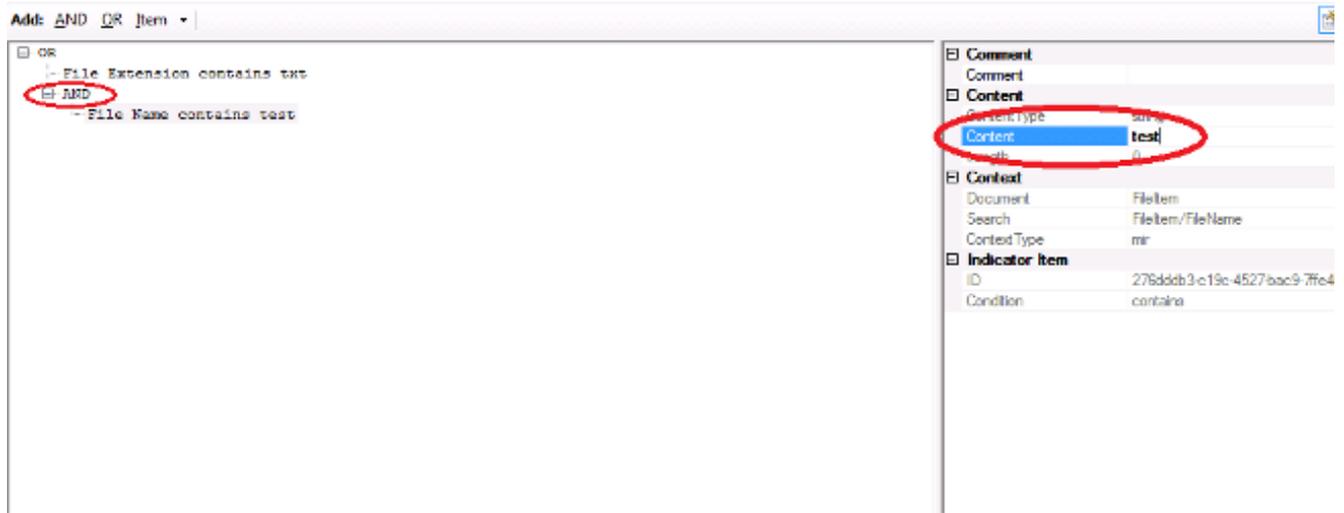


**Nota:** Per creare un IOC per un elemento specifico, utilizzare la logica binaria con le proprietà. L'operatore iniziale è un operatore OR, che è la base più semplice da utilizzare. In questo modo la funzione iniziale del COI è attiva e non è necessario modificarla. È necessario che un file di firma IOC disponga di almeno due proprietà o condizioni per poterlo utilizzare correttamente in un'analisi.

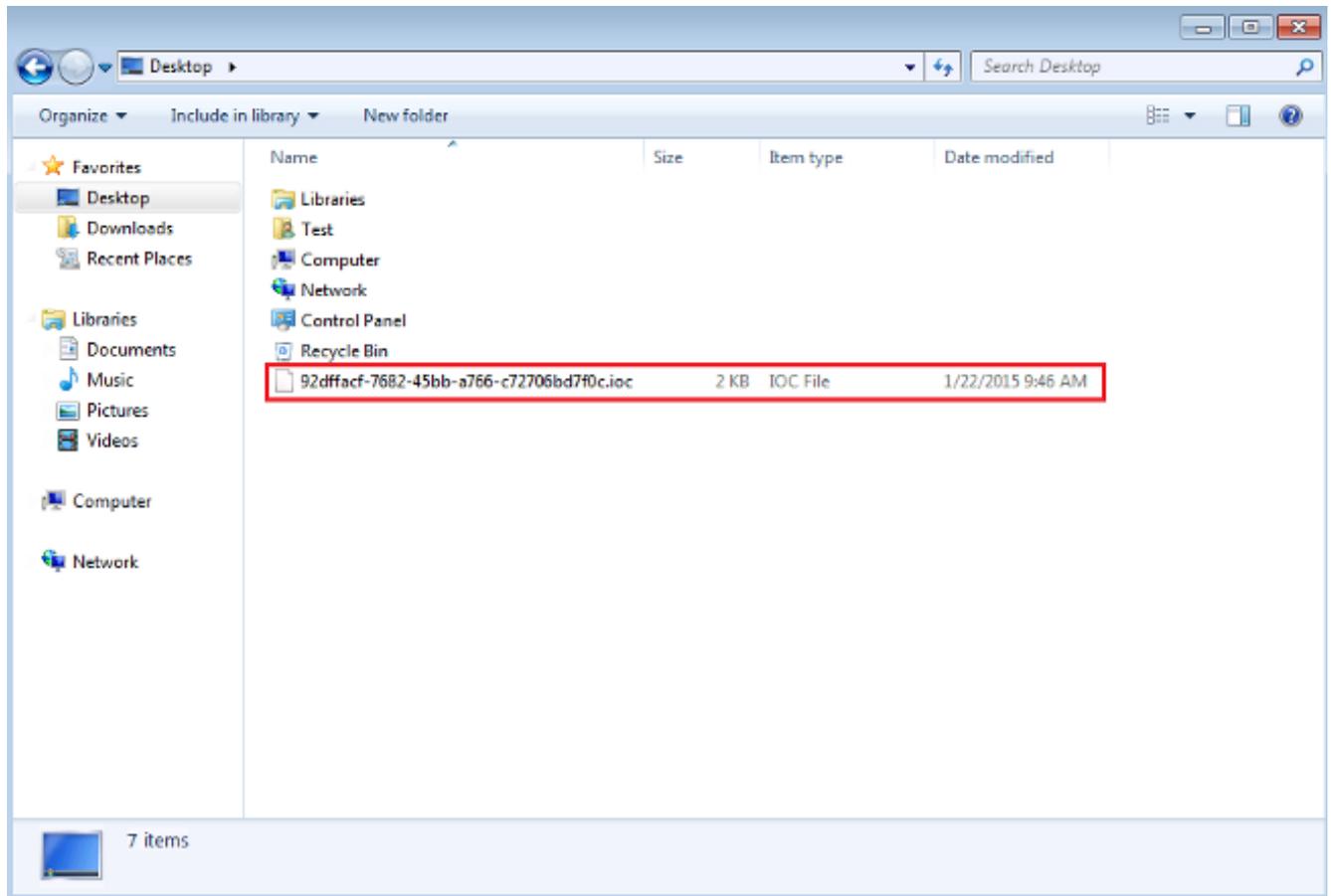
2. Per aggiungere operatori, fare clic sul menu a discesa **Items** (Elementi). La prima proprietà da aggiungere è **File Extension contiene**. Individuare la proprietà nel menu della struttura **Elementi** e fare clic su di essa.
3. Dopo aver aggiunto una proprietà, fare clic sull'icona piccola all'estrema destra dello schermo per aprire il riquadro Configurazione. In questo riquadro utilizzare il campo **Contenuto** in modo che corrisponda a un'estensione di file. Ad esempio, aggiungere **txt** in modo che corrisponda al file di testo **test.txt**:



4. A questo punto è necessario aggiungere un operatore logico. In questo esempio, verrà trovata una corrispondenza con il file di testo **di prova**. Per ottenere una corrispondenza, utilizzare un operatore **AND** e aggiungere la proprietà next. Individuare il nome del file e selezionarlo dal menu della struttura **Elementi**. Nel riquadro Proprietà aggiungere il nome del file che si desidera trovare. Ad esempio, aggiungere **test** nel campo Contenuto:



5. Poiché non sono necessarie proprietà aggiuntive per questo IOC semplice, è ora possibile salvare il file. Fare clic su **File > Salva** e viene salvato un file di firma con estensione **.ioc**:



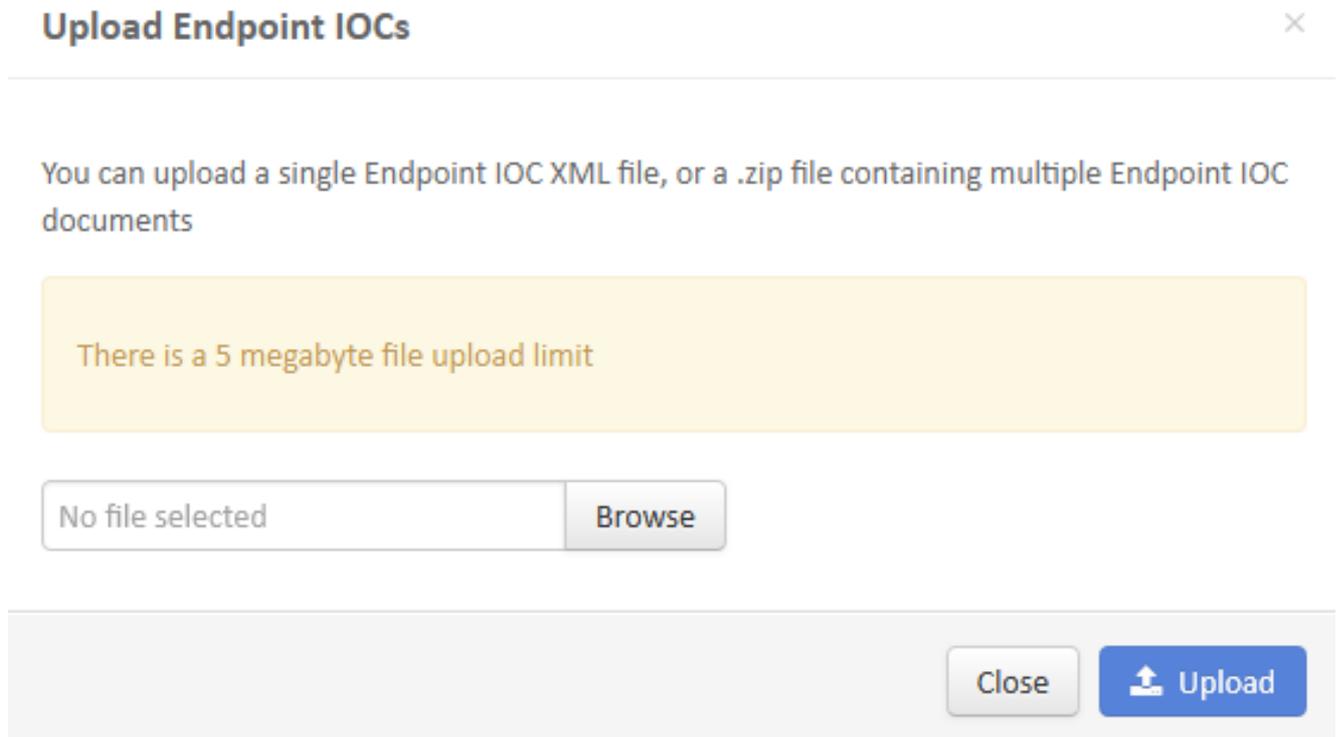
## Carica un file di firma IOC

Per eseguire una scansione, è necessario caricare un file IOC nel dashboard FireAMP. È possibile utilizzare un file di firma IOC, un file XML o un archivio zip contenente più file IOC. Il dashboard decompone e analizza il file con le firme IOC. Viene visualizzata una notifica se viene utilizzata una sintassi errata o una proprietà non supportata.

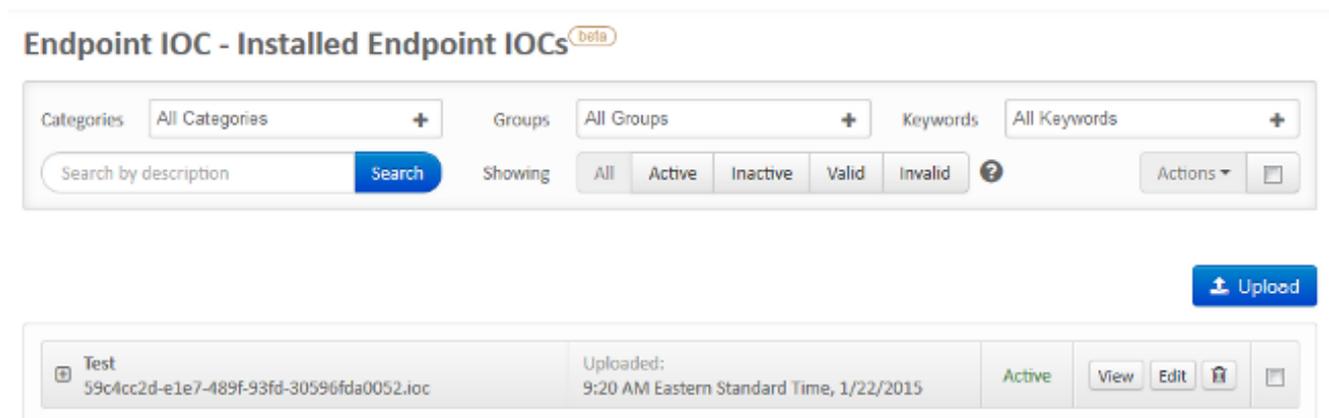
**Suggerimento:** È possibile caricare file di dimensioni fino a cinque megabyte.

Completare questi passaggi per caricare il file della firma IOC nel dashboard FireAMP:

1. Accedere alla console del cloud FireAMP e selezionare **Controllo epidemie > IOC endpoint installato**.
2. Fare clic su **Upload**. Viene visualizzata la finestra **Upload Endpoint IOCs**:



Una volta caricato correttamente un file di firma IOC, la firma viene visualizzata nell'elenco:



3. Per visualizzare i dati XML effettivi della firma, fare clic su **Visualizza**:

## 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>
```

## Avvia analisi

Dopo aver caricato un file di firma, eseguire un'analisi *completa*. La prima analisi deve essere completa, in quanto è necessario creare un catalogo di metadati per l'intero computer, operazione che può richiedere da 1 a 2 ore. È possibile eseguire una scansione *flash* dopo che il sistema è stato catalogato mediante una scansione completa.

**Nota:** La scansione completa richiede un uso intensivo della CPU. Cisco consiglia di non eseguire un'analisi completa su un PC mentre è in uso. Se si prevede di utilizzare questa funzione regolarmente, è possibile eseguire un'analisi completa una volta al mese per ricostruire il catalogo.

Per eseguire una scansione IOC è possibile utilizzare due metodi diversi. Il primo metodo consiste nell'eseguire un'analisi immediata da un evento o dal dashboard. Questo viene attivato la volta successiva che un PC invia un heartbeat al cloud.

**Nota:** Se è la prima volta che si esegue l'analisi completa, non è necessario controllare l'opzione **Ricarica prima dell'analisi**.

## 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

Il secondo metodo consiste nel creare una scansione IOC dell'endpoint pianificata dal menu **Controllo epidemie** del dashboard. Questa opzione è ideale quando si desidera eseguire scansioni durante le ore di minore utilizzo. Per creare attività pianificate e consentire l'autorizzazione **Accesso come** Criteri di gruppo **batch**, è necessario specificare le credenziali di un account che dispone dell'autorizzazione per il computer specificato.

## Endpoint IOC - Initiate Scan <sup>beta</sup>

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

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

Quando si pianifica un'analisi IOC dell'endpoint, viene visualizzato questo messaggio di avviso:

## 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

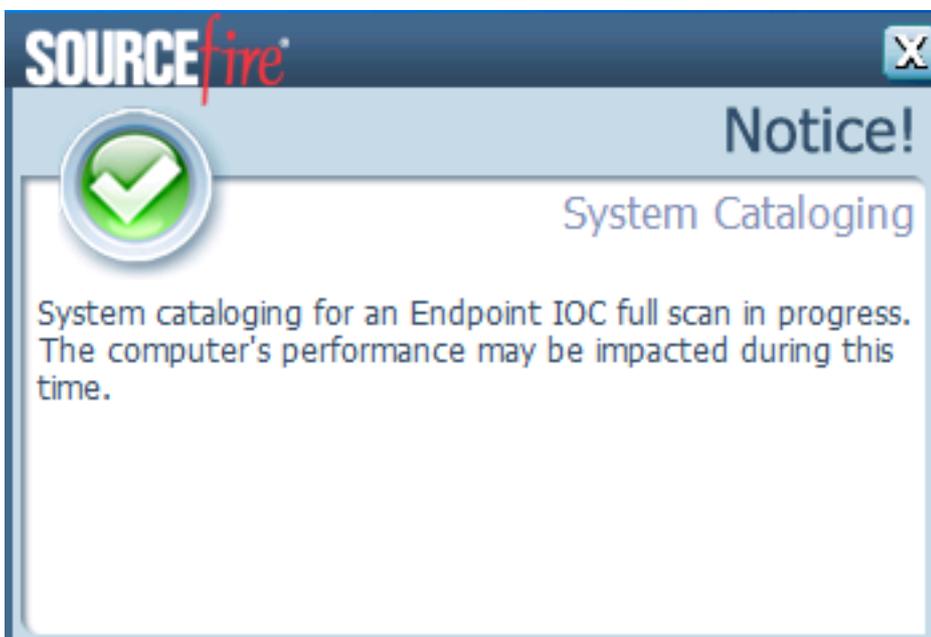
Schedule

Al successivo invio di un heartbeat dal PC e se le credenziali sono valide, nell'Utilità di pianificazione di Windows verrà visualizzato un processo simile al seguente:

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

All'inizio della scansione, viene visualizzato questo messaggio:

**Nota:** Se la GUI è configurata per essere nascosta, la notifica di **Catalogo di sistema** non viene visualizzata.



Al termine dell'analisi, sarà possibile visualizzare il *riepilogo di rilevamento analisi IOC endpoint*. Nell'esempio viene mostrata una corrispondenza per il file di firma 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  
Connector GUID: a0881bab-af05-402c-a7c8-0bf0824a6638  
Current User: [Redacted]

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]

View All