

Exécutez l'indication de point final des balayages de la compromission (COI) avec l'AMPÈRE pour des points finaux ou FireAMP

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Fichiers de signatures COI](#)

[Exécutez un balayage sur un fichier de signatures COI](#)

[Créez un fichier de signatures COI](#)

[Téléchargez un fichier de signatures COI](#)

[Initiez un balayage](#)

Introduction

Ce document décrit comment créer une indication de fichier de signatures de la compromission (COI) par l'intermédiaire de l'éditeur COI de Mandiant, comment le télécharger au tableau de bord de Cisco FireAMP, et comment initier un COI de point final balayez.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez au moins un giga de l'espace lecteur libre avant que vous tentiez d'exécuter les balayages COI de point final.

[Composants utilisés](#)

Les informations dans ce document sont basées sur le module de balayage COI de point final, qui est disponible dans les versions 4.0.2 et ultérieures de connecteur de Cisco FireAMP Windows.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-

vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

La caractéristique de scanner COI de point final est un outil puissant de réponse d'incident qui est utilisé afin de balayer des indicateurs de POST-compromission à travers de plusieurs ordinateurs.

Remarque: Bien que FireAMP prenne en charge l'iocs avec le langage de Mandiant, le logiciel d'éditeur COI de Mandiant lui-même n'est pas développé ou est pris en charge par Cisco. Cisco les prennent en charge ne dépanne pas créé par l'utilisateur ou la tierce partie iocs.

Fichiers de signatures COI

Le fichier de signatures COI est un schéma XML extensible pour la description des caractéristiques techniques qui identifient une menace connue, une méthodologie d'attaquant, ou d'autres preuves de compromission.

Vous pouvez importer le point final iocs par la console des fichiers basés sur OpenIOC qui sont écrits afin de déclencher sur des propriétés de fichier telles que le nom, la taille, et les informations parasites, aussi bien que d'autres attributs et propriétés de système telles que les informations sur le processus, des services courants, et des entrées dans le registre de Microsoft Windows. La syntaxe COI peut être utilisée par des responders d'incident afin de trouver les objets façonnés spécifiques ou afin d'employer la logique pour créer des détections sophistiquées et corrélées pour des familles de malware.

Exécutez un balayage sur un fichier de signatures COI

Il y a trois étapes que vous devez se terminer afin d'exécuter un balayage sur un fichier de signatures COI :

1. Créez un fichier de signatures COI.
2. Téléchargez le fichier de signatures COI.
3. Initiez un balayage.

Ces étapes sont développées au moment dans les sections qui suivent.

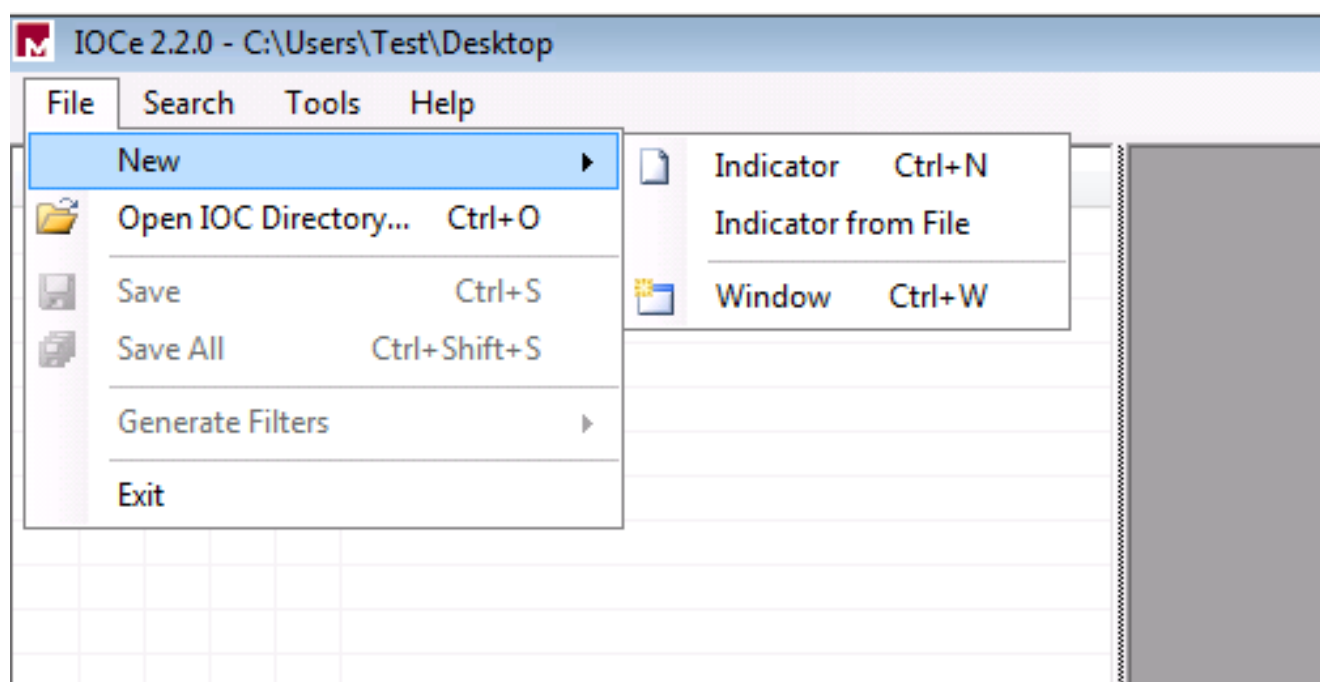
Créez un fichier de signatures COI

Remarque: Dans cet exemple, l'éditeur COI de Mandiant est utilisé afin d'établir un fichier de signatures COI pour un fichier texte nommé **test.txt**.

Terminez-vous ces étapes afin de créer un fichier de signatures COI :

1. Ouvrez l'IOCe et naviguez pour classer > nouveau > indicateur. Ceci fournit un espace de

travail vide de sorte que vous puissiez commencer à construire un COI.



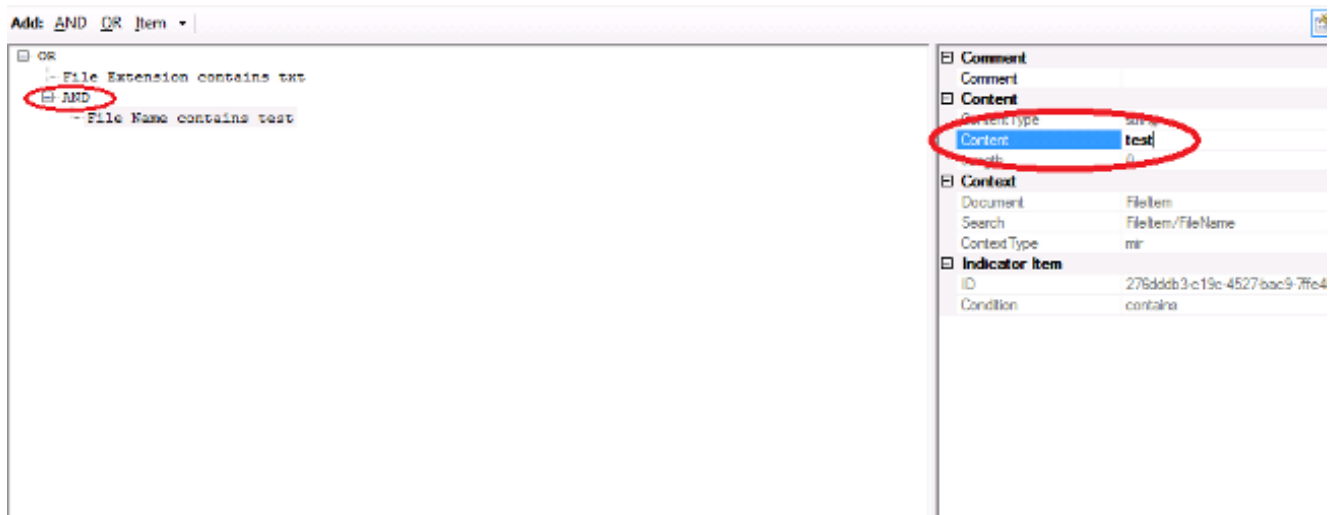
Remarque: Afin de créer un COI pour quelque chose spécifique, utilisez la logique binaire avec les propriétés. L'opérateur initial est donc OU, est la base la plus simple à fonctionner. Ceci permet à la fonction initiale du COI pour fonctionner, ainsi vous n'êtes pas requis de la changer. On l'exige qu'un fichier de signatures COI a au moins deux propriétés ou conditions afin de l'utiliser avec succès dans un balayage.

2. Cliquez sur le menu déroulant d'**éléments** afin d'ajouter des opérateurs. La première propriété que vous devriez ajouter est **extension de fichier contient**. Trouvez la propriété dans le menu d'arborescence d'**éléments** et cliquez sur-la.
3. Après que vous ajoutiez une propriété, cliquez sur la petite icône du côté droit le côté d'extrême droite de l'écran afin d'ouvrir le volet de configuration. Dans ce volet, employez le champ **satisfait** afin d'apparier une extension de fichier. Par exemple, ajoutez le **txt** afin de sélectionner le fichier texte de **test.txt** :

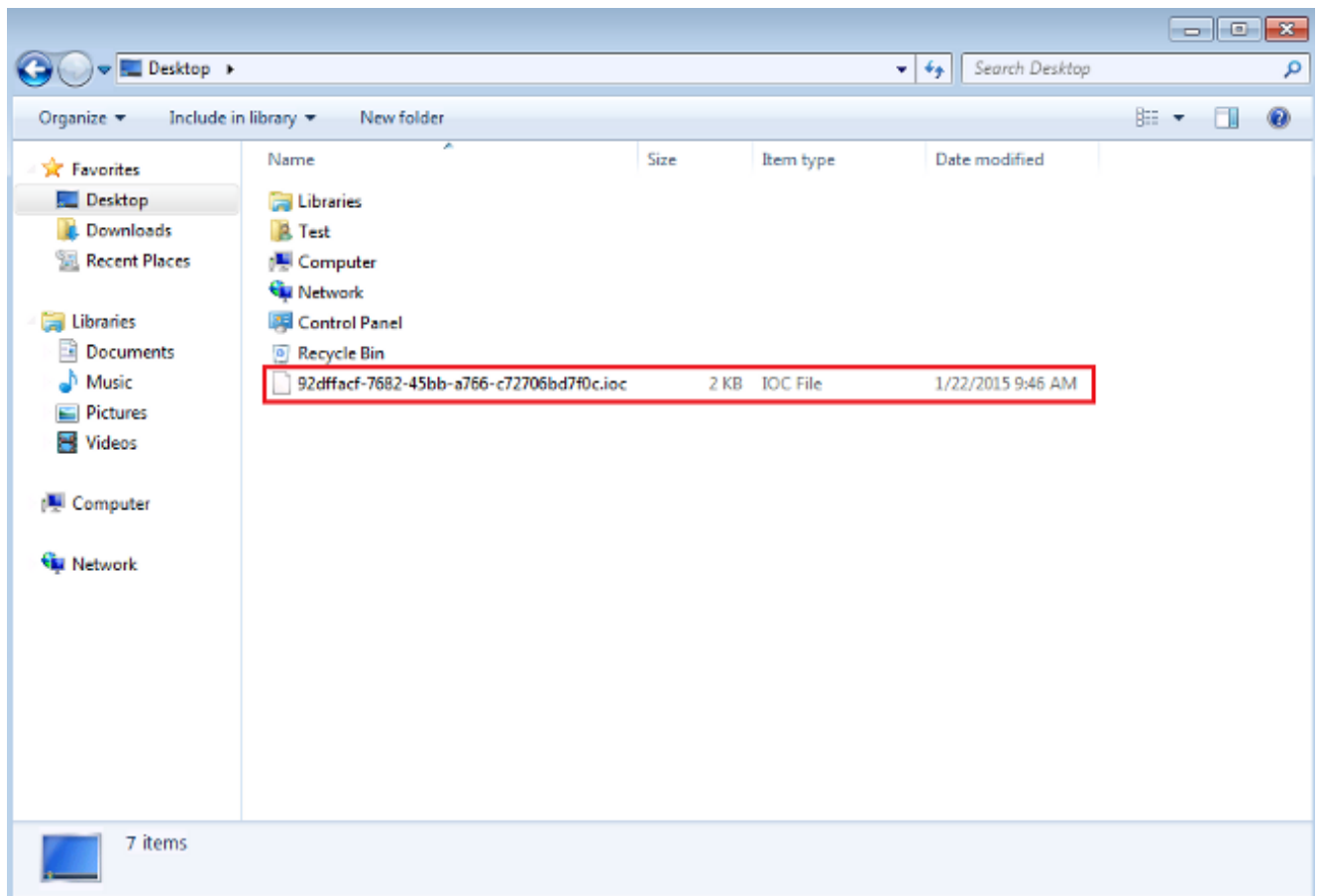


4. Vous devez maintenant ajouter un opérateur de logique. Dans cet exemple, vous sélectionnez le fichier de **texte d'essai**. Afin d'apparier ceci, utilisez **ET** l'opérateur et ajoutez la prochaine propriété. Localisez le nom du fichier et sélectionnez-le du menu d'arborescence d'**éléments**. Dans le volet de Properties, ajoutez le nom du fichier que vous

voulez pour le trouver. Par exemple, ajoutez le **test** dans le domaine satisfait :



5. Puisqu'aucune propriété supplémentaire n'est nécessaire pour ce COI simple, vous pouvez maintenant sauvegarder le fichier. **Le fichier > la sauvegarde de clic**, et un fichier de signatures avec une extension **.ioc** est enregistré sur le système :



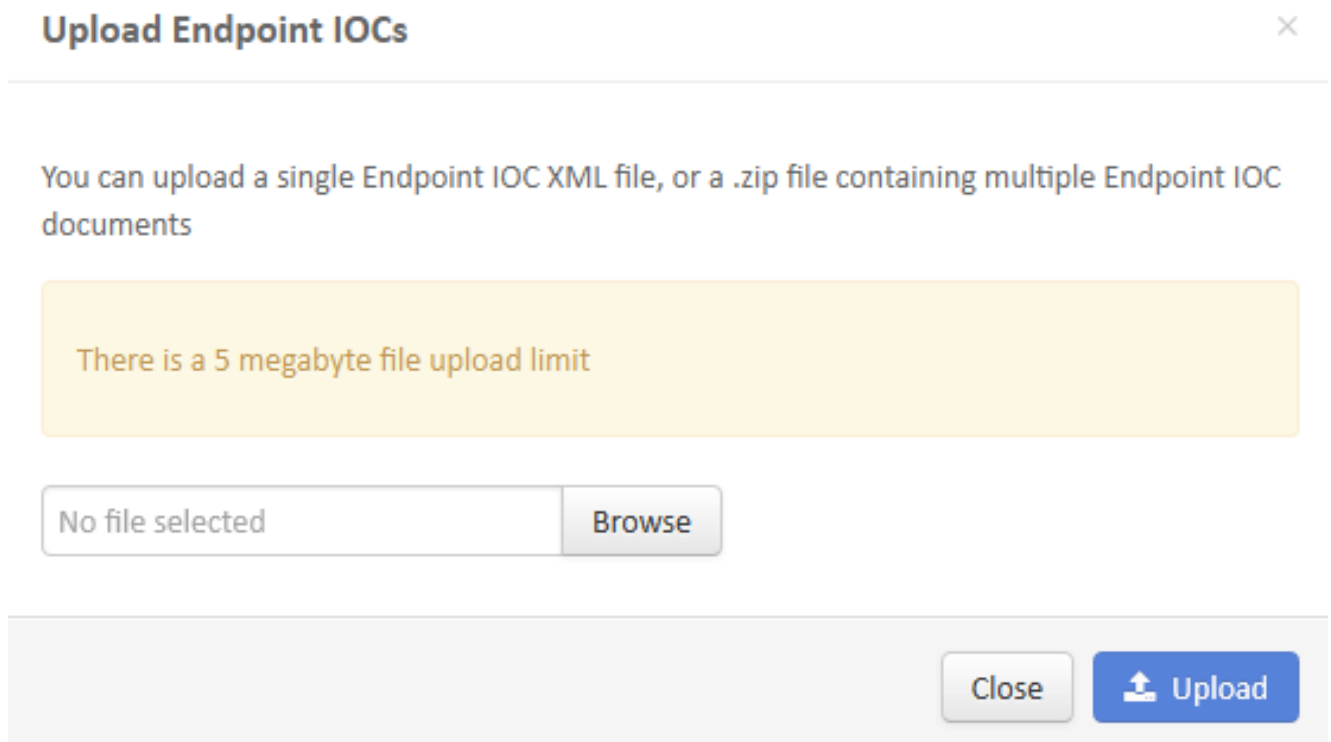
Téléchargez un fichier de signatures COI

Afin d'exécuter un balayage, vous devez télécharger un COI classé au tableau de bord de FireAMP. Vous pouvez utiliser un fichier de signatures COI, un fichier XML, ou des archives de zip qui contiennent de plusieurs fichiers COI. Le tableau de bord décompresse et analyse le fichier avec les signatures COI. On vous annonce si une syntaxe incorrecte ou une propriété non vérifiée est utilisée.

Conseil : Vous pouvez télécharger les fichiers qui sont jusqu'à cinq mégaoctets dans la taille.

Terminez-vous ces étapes afin de télécharger le fichier de signatures COI au tableau de bord de FireAMP :

1. Connectez-vous dans la console de nuage de FireAMP et naviguez vers le **contrôle d'épidémie > COI installé de point final**.
2. Cliquez sur Upload, et la fenêtre du **point final iocs de téléchargement** apparaît :



Upload Endpoint IOCs ×

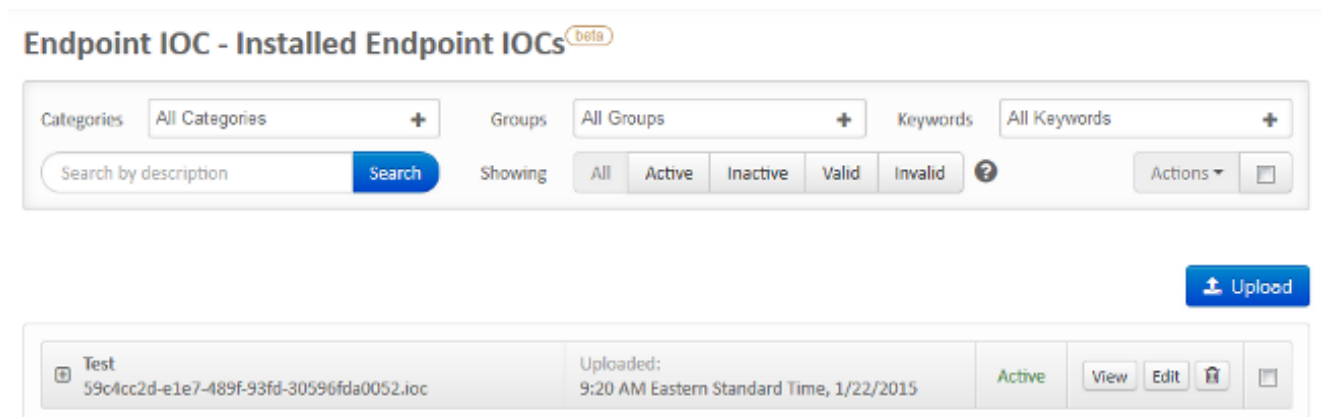
You can upload a single Endpoint IOC XML file, or a .zip file containing multiple Endpoint IOC documents

There is a 5 megabyte file upload limit

No file selected Browse

Close Upload

Après qu'un fichier de signatures COI soit téléchargé avec succès, la signature apparaît sur la liste :



Endpoint IOC - Installed Endpoint IOCs beta

Categories + Groups + Keywords +

Search Showing ? Actions ▾ 🗑️

Upload

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

3. Cliquez sur la **vue** afin de visualiser les données XML réelles de la signature :

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      <IndicatorItem id="6ac73c61-9e9f-43da-9317-38d09990c337" condition="contains">
16        <Context document="FileItem" search="FileItem/FileName" type="mir" />
17        <Content type="string">test</Content>
18      </IndicatorItem>
19    </Indicator>
20  </definition>
21 </ioc>
```

Initiez un balayage

Après que vous téléchargez un fichier de signatures, exécutez un *plein* balayage. Le premier balayage doit être un plein balayage parce qu'il doit construire un catalogue des métadonnées pour l'ordinateur entier, qui peut prendre 1 – 2 heures. Vous pouvez exécuter un balayage *instantané* après que le système soit catalogué par un plein balayage.

Remarque: Le plein balayage est très CPU intensive. Cisco recommande que vous n'exécutiez pas un plein balayage sur un PC tandis qu'il est en service. Si vous prévoyez d'utiliser la caractéristique régulièrement, vous pouvez exécuter un plein balayage une fois par mois afin de reconstruire le catalogue.

Il y a deux différentes méthodes que vous pouvez employer afin de diriger un COI balayez. La première méthode est d'exécuter un balayage immédiat d'un événement ou du tableau de bord. Ceci est déclenché la prochaine fois qu'un PC envoie à une pulsation au nuage.

Remarque: Si c'est la première fois que vous exécutez le plein balayage, vous n'êtes pas requis de vérifier le **recatalogage** avant l'option de **balayage**.

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

La deuxième méthode est de créer un COI programmé de point final balayent du menu de **contrôle d'épidémie** du tableau de bord. Cette option pourrait être idéale quand vous désirez exécuter des balayages pendant des heures creuses. Vous devez fournir les qualifications d'un compte qui a l'autorisation sur l'ordinateur donné afin de créer des tâches programmées et permettre le **login en tant qu'**autorisation de stratégie de groupe **en lots**.

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

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

Quand vous programmez un balayage COI de point final, ce message d'avertissement apparaît :

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

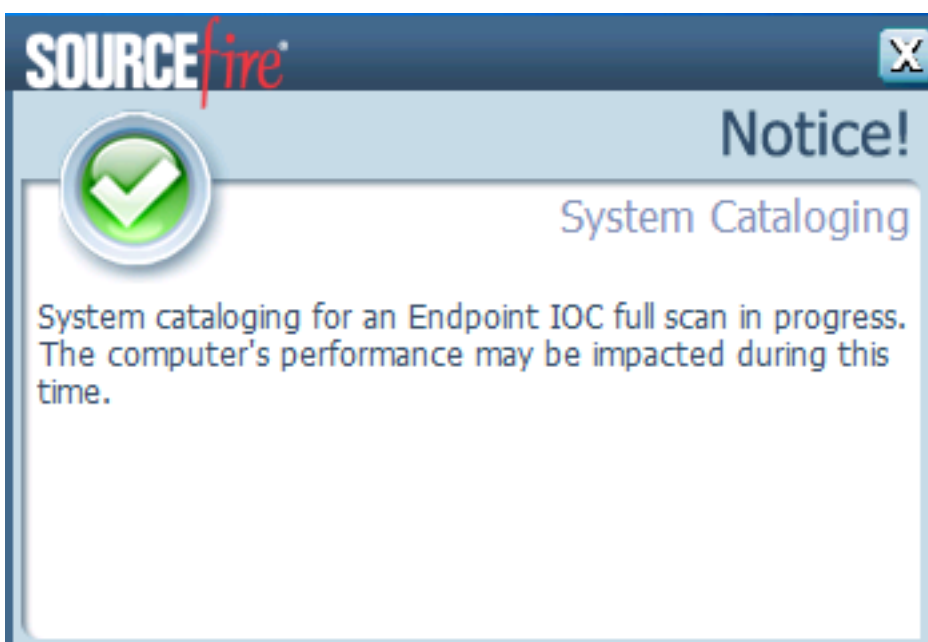
Schedule

La prochaine fois que ce votre PC envoie une pulsation, et si vos qualifications sont valides, vous devriez voir un travail semblable à ceci dans le programmeur de tâche de 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

Quand le balayage commence, ce message apparaît :

Remarque: Si le GUI est configuré pour être masqué, alors vous ne voyez pas l'avis cataloguant de système.



Quand le balayage est complet, vous pouvez visualiser le *COI de point final* analysez le *résumé de détection*. Cet exemple affiche une correspondance pour le fichier de signatures COI de **test.txt** :

The screenshot displays two panels from a security management interface. 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 "a088bbab-ef05-402c-e7c8-6bf0824e6638" and includes a "Run Scan" button. The bottom panel, titled "Win7 Endpoint IOC Scan Detection Summary (matched 1 of 1 IOCs)", shows a single detection: "Test [Filename: 59c4cc2d-e1a7-489f-93fd-3059685a0052.ioc]". It includes a "View All" button and a "Launch Device Trajectory" button in the top right corner of the interface.

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:	a088bbab-ef05-402c-e7c8-6bf0824e6638	
	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-e1a7-489f-93fd-3059685a0052.ioc]	
Connector Info			
Comments	View All		