

エンドポイント向け AMP または FireAMP で Endpoint Indication of Compromise (IOC) スキャンを実行する

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[IOC 署名 ファイル](#)

[IOC 署名 ファイルのスキャンをして下さい](#)

[IOC 署名 ファイルを作成して下さい](#)

[IOC 署名 ファイルをアップロードして下さい](#)

[スキャンを始めて下さい](#)

概要

この資料に Mandiant IOC エディタで侵害 (IOC) 署名 ファイルの示す値を、Cisco FireAMP ダッシュボードにそれを作成する方法をおよびエンドポイント IOC スキャンをアップロードする方法を始める方法を記述されています。

前提条件

要件

Cisco はエンドポイント IOC スキャンをするように試みる前に自由なドライブ領域の少なくとも 1 ギガバイトがあることを推奨します。

使用するコンポーネント

この文書に記載されている情報は Cisco FireAMP Windows コネクタ バージョン 4.0.2 および それ以降で利用可能であるエンドポイント IOC スキャンナーに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく

必要があります。

背景説明

複数のコンピューターを渡る後侵害インジケータをスキャンするために使用するエンドポイント IOC スキャナー機能は強力なインシデント レスポンス ツールです。

注: FireAMP が Mandiant 言語の IOC をサポートするが、Mandiant IOC エディタ ソフトウェア自体は Cisco によって開発されませんし、サポートされません。Cisco サポートはユーザー定義サードパーティ IOC を解決しません。

IOC 署名 ファイル

IOC 署名 ファイルは侵害の既知 脅威、攻撃者 方法論、または他の証拠を識別する技術特性の説明のための拡張可能な XML スキーマです。

名前のようなファイル プロパティで、サイズおよびハッシュ引き起こすために書かれている、またプロセス 情報のような他の属性およびシステム 性質できま OpenIOC ベースのファイルからコンソールによってエンドポイント IOC を、サービス インポートおよび Microsoft Windows レジストリエントリを実行します。IOC 構文は事件レスポンスによって特定の成果物を見つけるためにまたは malware の系列のための洗練された、関連させた検出を作成するのにロジックに従うために使用することができます。

IOC 署名 ファイルのスキャンをして下さい

IOC 署名 ファイルのスキャンをするために完了する必要がある 3 つのステップがあります:

1. IOC 署名 ファイルを作成して下さい。
2. IOC 署名 ファイルをアップロードして下さい。
3. スキャンを始めて下さい。

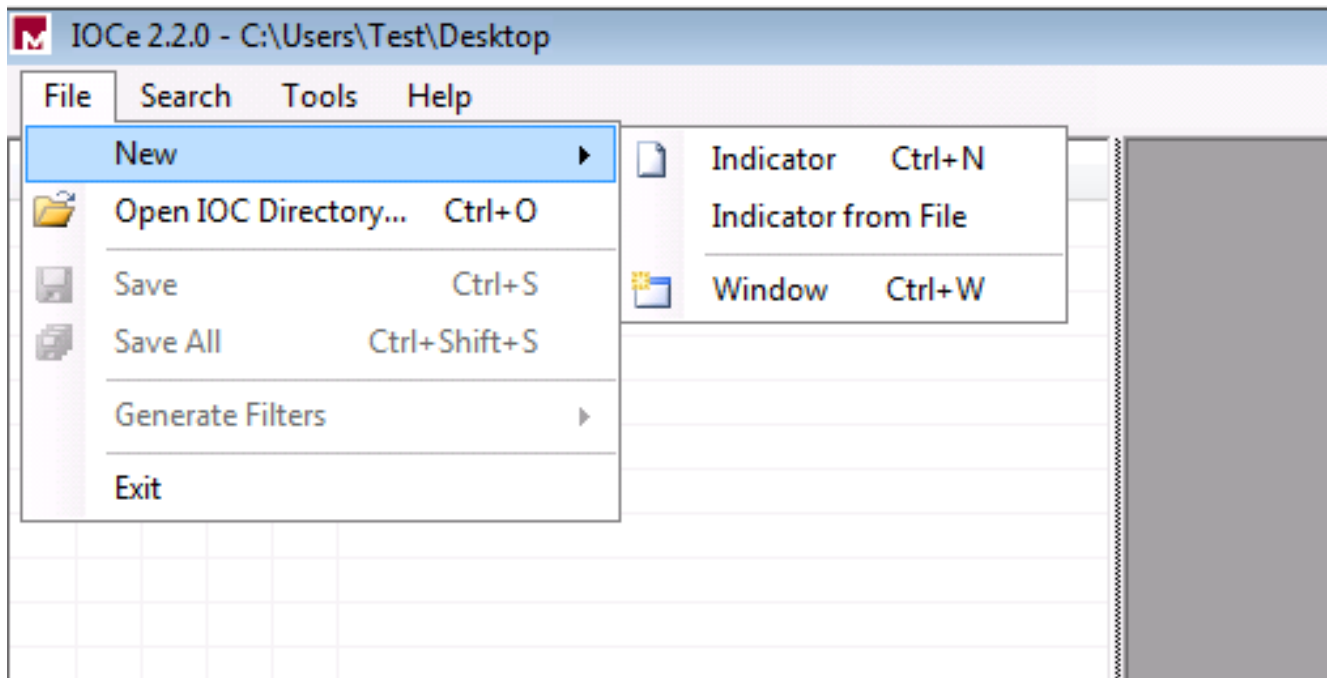
これらのステップは続くセクションで説明されます。

IOC 署名 ファイルを作成して下さい

注: この例では `test.txt` と名付けられるテキストファイルのための IOC 署名 ファイルを構築するために、Mandiant IOC エディタは使用されます。

IOC 署名 ファイルを作成するためにこれらのステップを完了して下さい:

1. IOCe を開き、**File > New > インジケータ**にナビゲートして下さい。これは IOC を構築し始めることができるようにブランク ワークスペースを提供します。

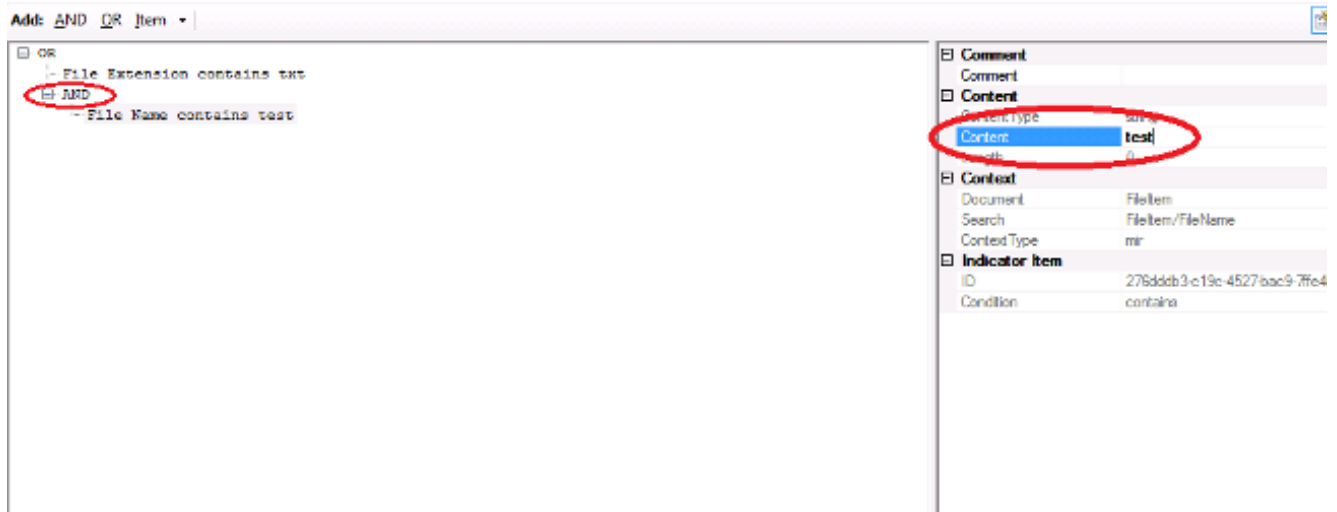


注: 特定の何かのための IOC を作成するためにプロパティとバイナリ ロジックに従って下さい。はたらく最も簡単なベースがある最初のオペレータはまたはです。これは IOC の最初の機能がはたらくようにします従ってそれを変更するために必要となりません。スキャンでそれを正常に使用するために IOC 署名 ファイルに少なくとも 2 プロパティが条件があることが必要となります。

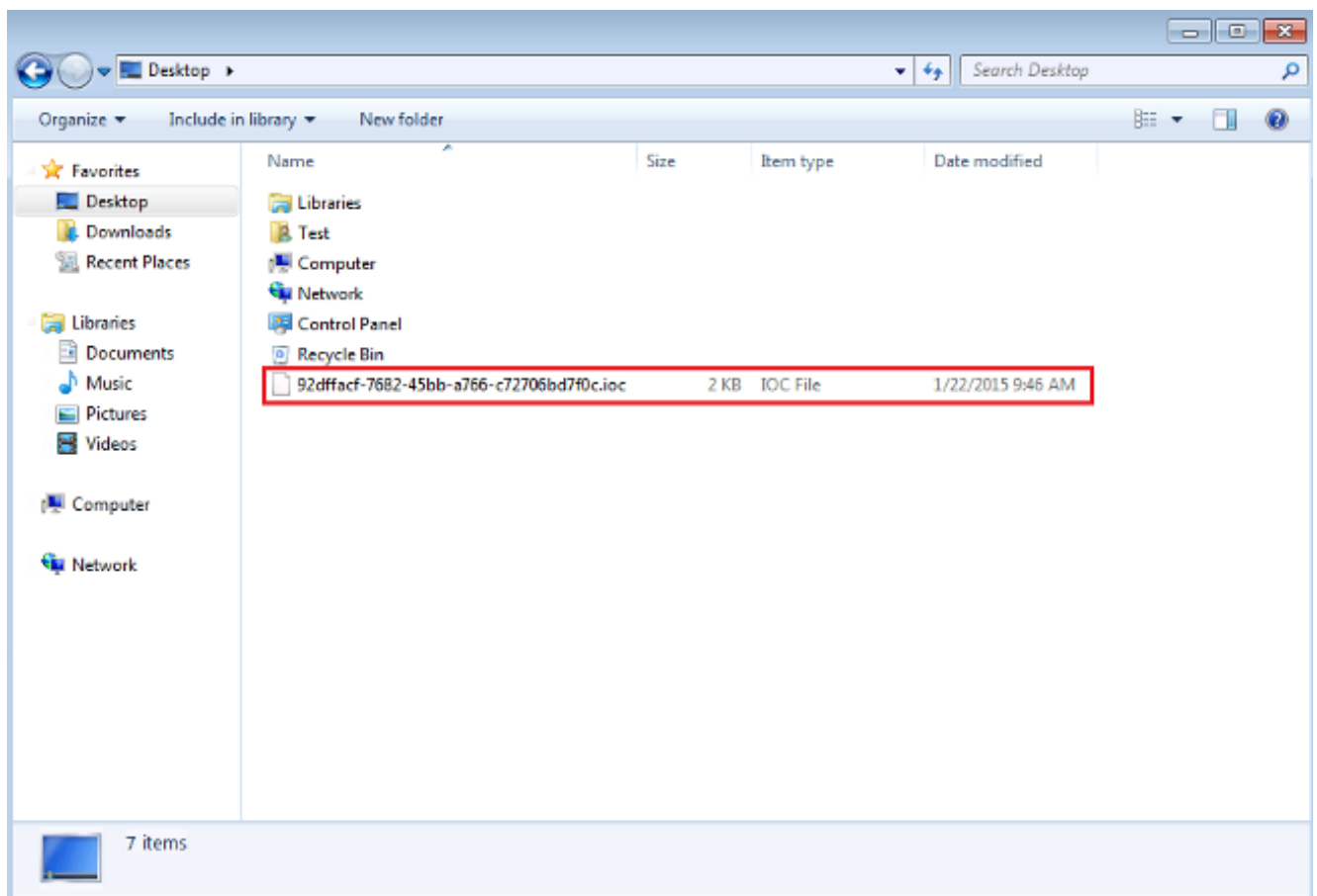
2. オペレータを追加するために項目ドロップダウン メニューをクリックして下さい。追加する必要がある最初のプロパティはファイル拡張子含んでいます。項目ツリーメニューのプロパティを見つけ、クリックして下さい。
3. プロパティを追加した後、設定 ペインを開くために画面の右端の小さいアイコンをクリックして下さい。このペインの中では、ファイル拡張子を一致するためにコンテンツ フィールドを使用して下さい。たとえば、**test.txt** テキストファイルを一致するために **txt** を追加して下さい:



4. 今ロジック オペレータを追加して下さい。この例では、テスト テキストファイルを一致する。これを一致するために、およびオペレータを使用し、次のプロパティを追加して下さい。ファイル名を見つけ、項目ツリーメニューから選択して下さい。プロパティ ペインでは、見つけたいと思うファイルの名前を追加して下さい。たとえば、コンテンツ フィールドのテストを追加して下さい:



- 追加のプロパティがこの簡単な IOC に必要ではないので、今ファイルを保存することができます。File > Save の順にクリックすれば、.ioc 拡張を用いる署名ファイルはシステムで保存されます:



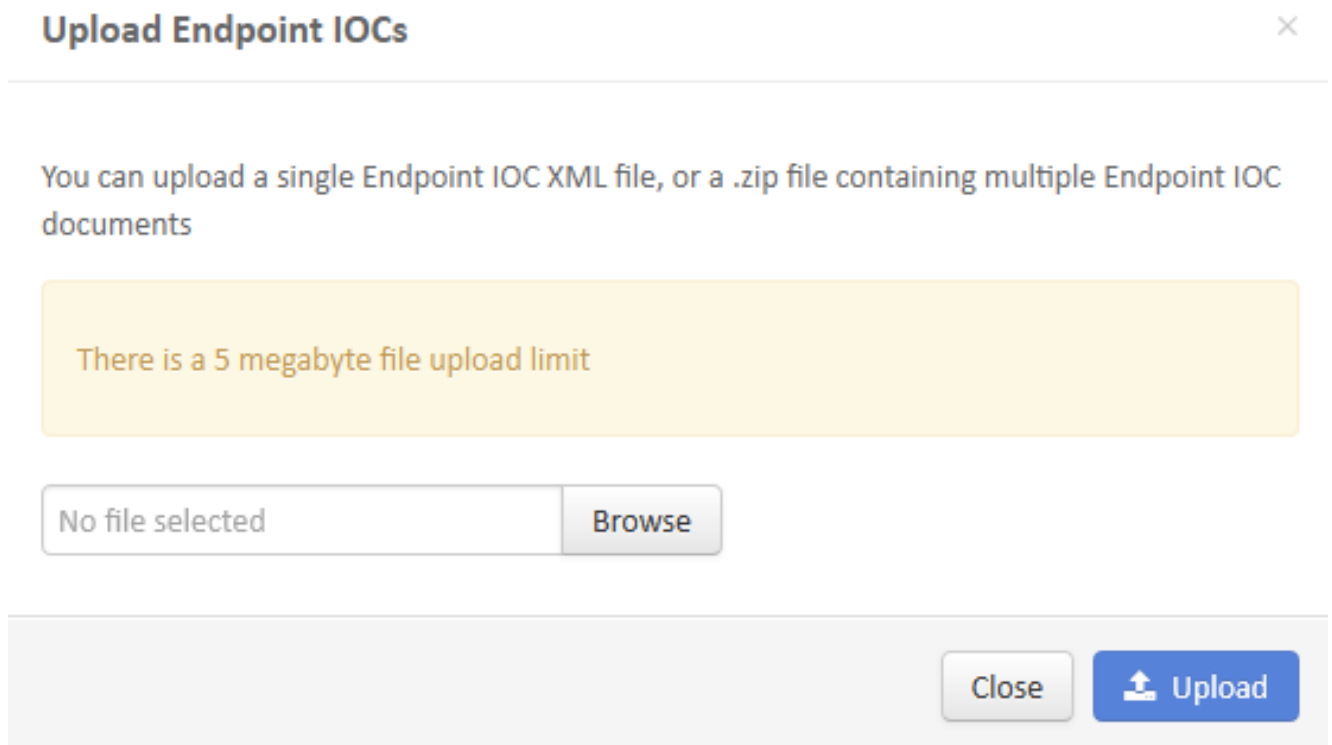
IOC 署名 ファイルをアップロードして下さい

スキャンを行うために、FireAMP ダッシュボードに IOC ファイルをアップロードして下さい。複数の IOC ファイルが含まれている IOC 署名 ファイル、XML ファイルを、または zip アーカイブを使用できます。ダッシュボードは IOC シグニチャとのファイルを復元し、解析します。不適切な構文がサポートされていないプロパティが使用される場合知らされます。

ヒント：5 メガバイトまでであるファイルをアップロードできます。

FireAMP ダッシュボードに IOC 署名 ファイルをアップロードするためにこれらのステップを完了して下さい:

1. FireAMP Cloud コンソールにログイン し、発生コントロールに > インストール済みエンドポイント IOC ナビゲート して下さい。
2. 『Upload』 をクリック すれば、アップロード エンドポイント IOC ウィンドウは現われます:



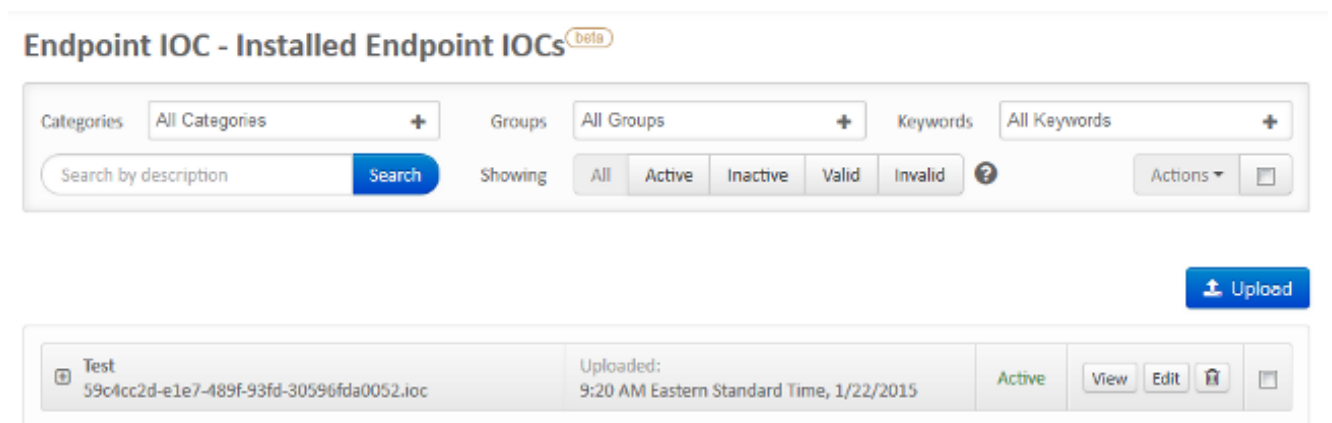
Upload Endpoint IOCs ×

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

IOC 署名 ファイルが正常にアップロードされた後、シグニチャはリストで現われます:



Endpoint IOC - Installed Endpoint IOCs ^{beta}

Categories: All Categories Groups: All Groups Keywords: All Keywords

Search by description Showing: All Active Inactive Valid Invalid Actions

<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="☰"/>
---	---	--------	-------------------------------------	-------------------------------------	---------------------------------------	----------------------------------

3. シグニチャの実際の XML データを表示するために 『View』 をクリック して下さい:

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="2015-01-22T14:16:48" 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>
```

スキャンを始めて下さい

署名 ファイルをアップロードした後、完全なスキャンを行って下さい。最初のスキャンは 1-2 時間がかかる場合がある全体のコンピュータのためのメタデータのカタログを構築する必要があるため完全なスキャンである必要があります。システムが完全なスキャンによってカタログされた後フラッシュスキャンを行うことができます。

注: 完全なスキャンは非常に CPU 中心です。Cisco は使用中の間、PC の完全なスキャンをしないことを推奨します。機能を常用するために計画する場合カタログを再製するために完全なスキャンを月に一度行うことができます。

IOC スキャンをするために使用できる 2 つの異なった方法があります。最初の方式はイベントまたはダッシュボードからの即時スキャンを行うことです。PC が Cloud にハートビートを送信するこれは次に引き起こされます。

注: 完全なスキャンをすることこれが最初になら、スキャン オプションの前に再カタログをチェックするために必要となりません。

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2方式はダッシュボードの発生コントロールメニューからのスケジュールされたエンドポイント IOC スキャンを作成することです。このオプションはオフピークの時間間にスキャンを行うことを望むとき理想的であるかもしれませんが。特定のコンピューターの権限が Scheduled Tasks を作成し、ログインをバッチグループポリシー権限として許可するためにあるアカウントの資格情報を提供して下さい。

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

エンドポイント IOC スキャンをスケジュールするとき、この警告メッセージが現れます:

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

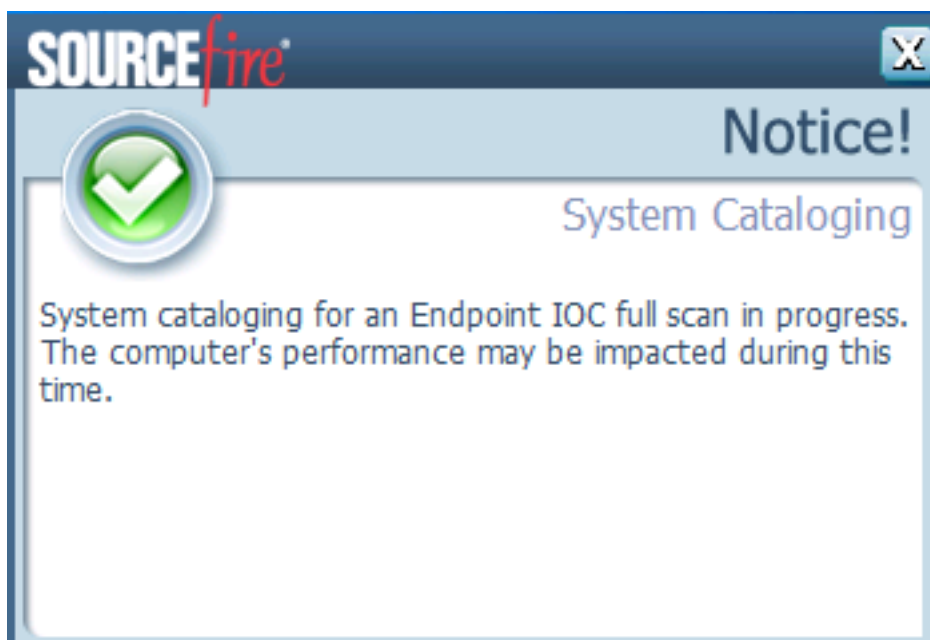
Schedule

その PC がハートビートを送信 する時次に、そして資格情報が有効なら、Windows タスク スケジューラでこれと同じようなジョブを見るはずです:

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

スキャンが始まるとき、このメッセージが現れます:

注: GUI が非表示であるために設定される場合システムが表記をカタログすることを見ません。



スキャンが完了するとき、エンドポイント IOC スキャン 検出 要約を表示できます。この例は test.txt IOC 署名 ファイルのための一致を示したものです:

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-a7c8-0bf0824a6638	
	Current User:		
	Run Scan		Launch Device Trajectory
Win7 Endpoint IOC Scan Detection Summary (matched 1 of 1 IOC)		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	View All		
Comments			