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

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ー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かサード 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 プロパティーで、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ダー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口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。

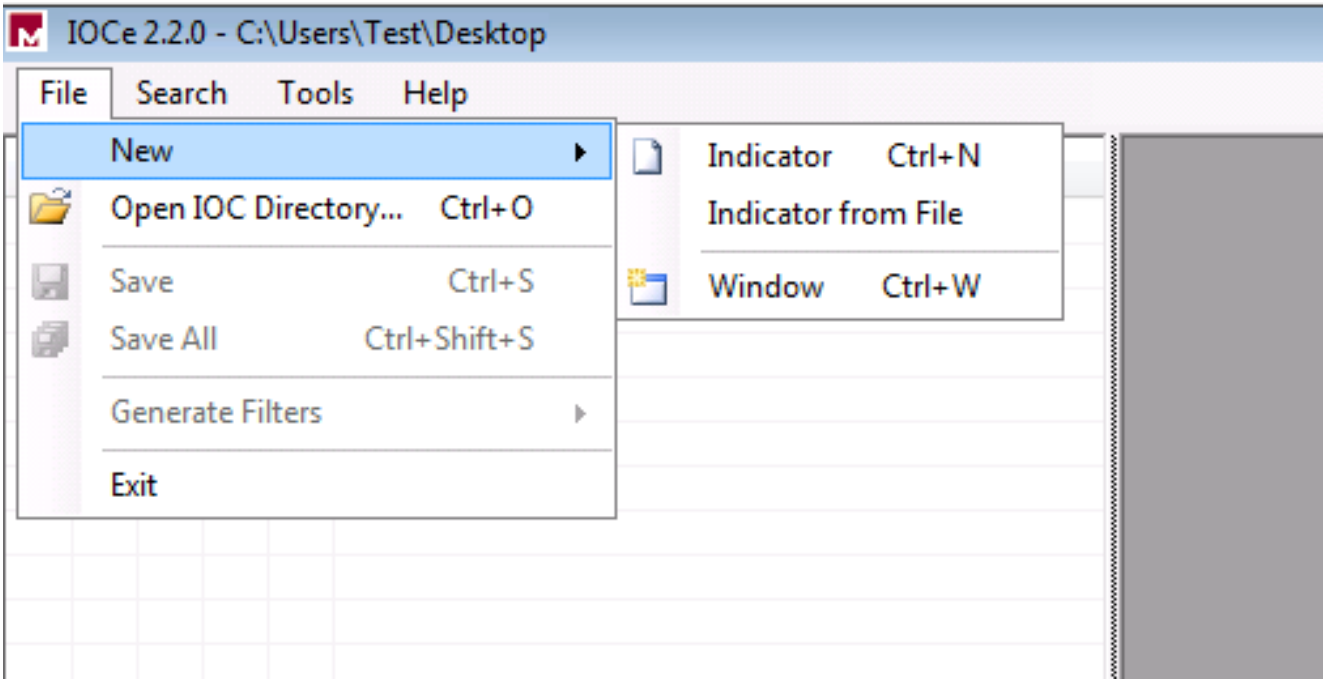
これらのステップは続くセクションで説明されます。

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:

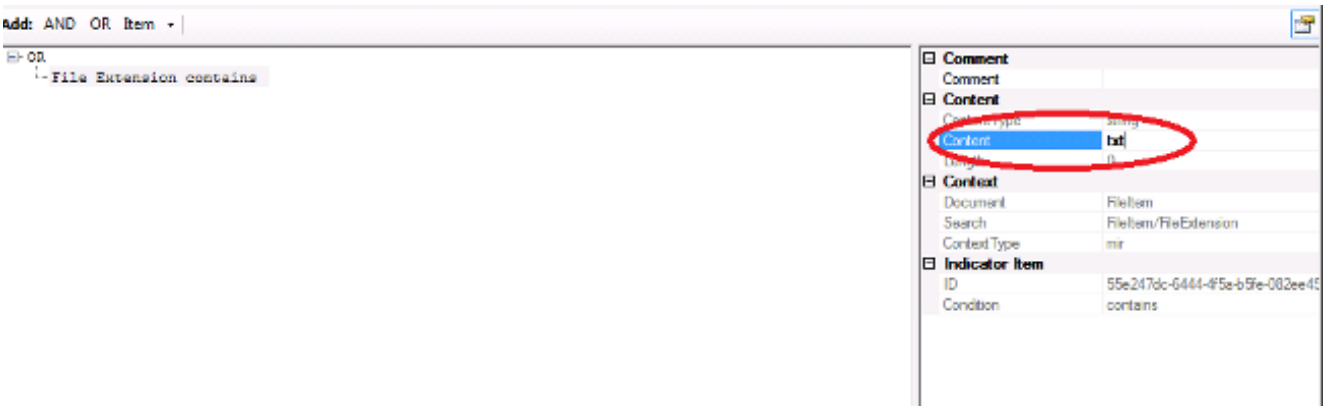
1. **IOCe を**開き、**File > New > インジケータ**にナビゲート して下さい。 これは IOC を構築し始めることができるようにブランク ワークスペースを提供します。



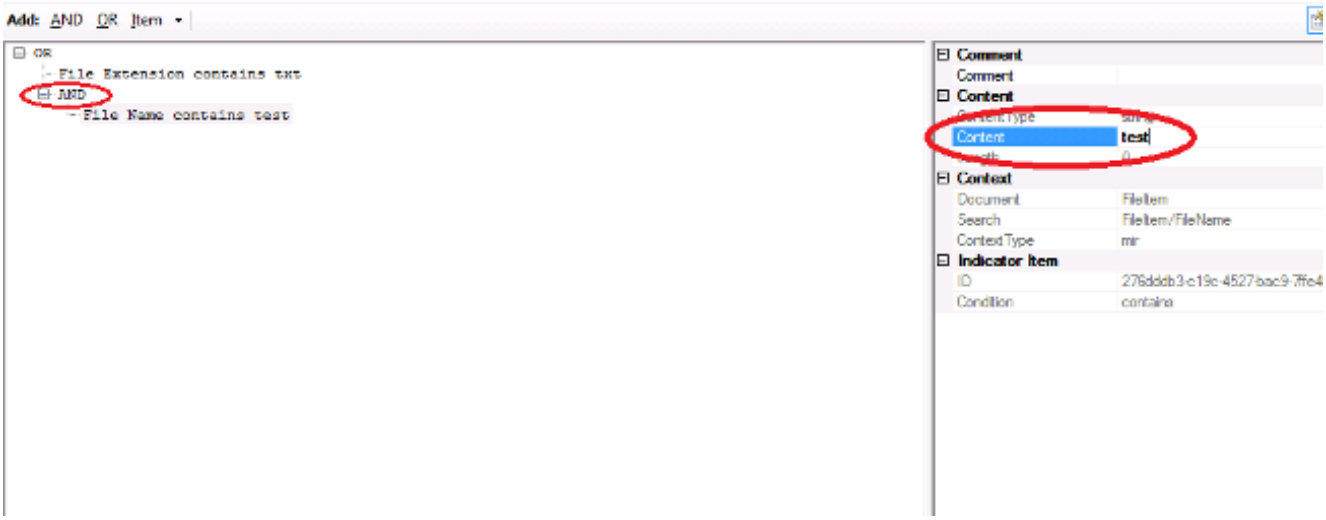
注: 特定の何かのための IOC を作成するためにプロパティとバイナリ ロジックに従って下さい。 はたらく最も簡単なベースがある最初のオペレータはまたはです。 これは IOC の最初の機能がはたらくようにします従ってそれを変更するために必要となりません。 スキャンでそれを正常に使用するために IOC 署名 ファイルに少なくとも 2 プロパティか条件があることが必要となります。

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**です。 **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。

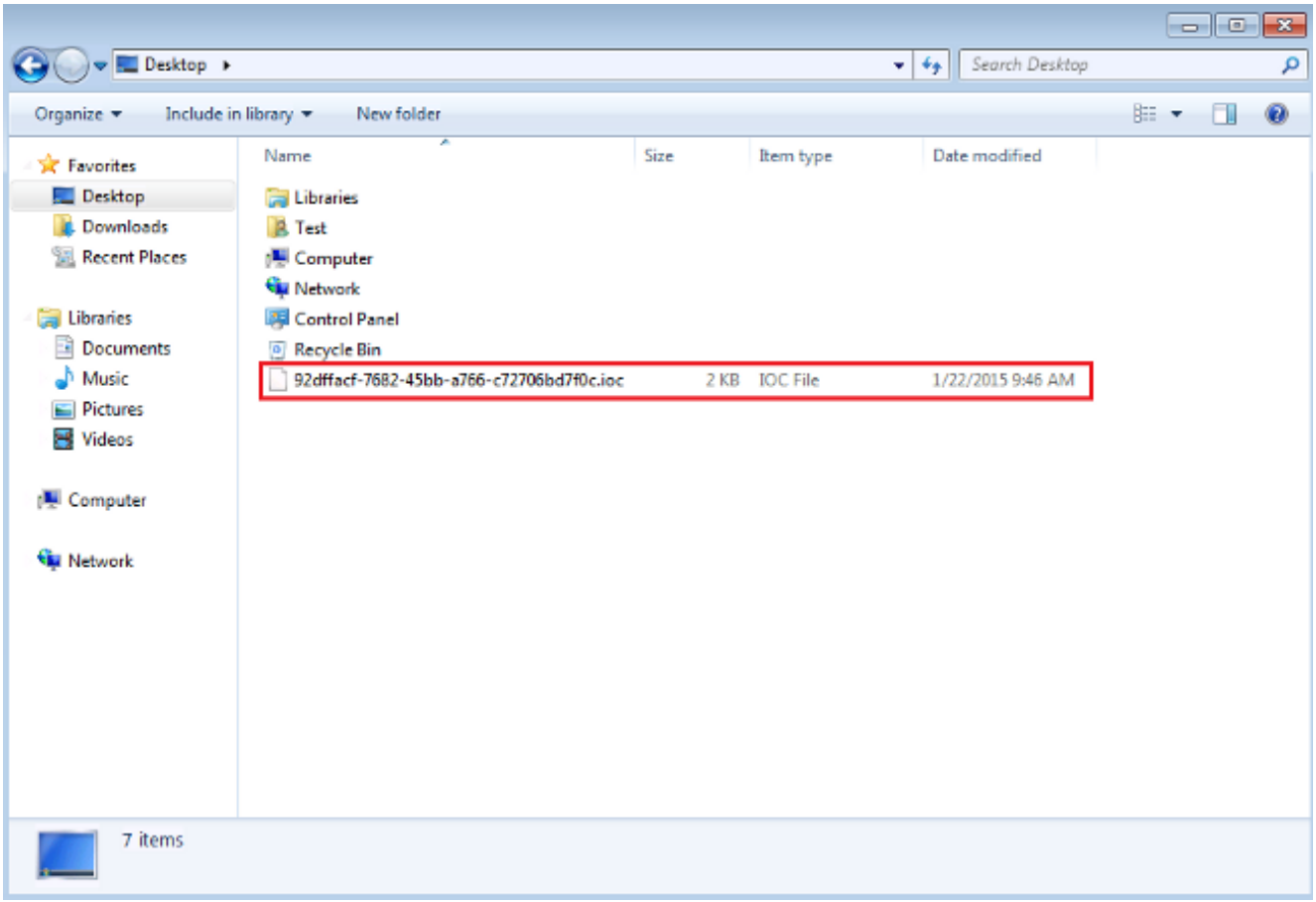
3. プロパティを追加した後、設定 ペインを開くために画面の右端の小さいアイコンをクリックして下さい。 このペインの中では、ファイル拡張子を一致するために**コンテンツ** フィールドを使用して下さい。 たとえば、**test.txt** テキストファイルを一致するために **txt を**追加して下さい:



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:



5. 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

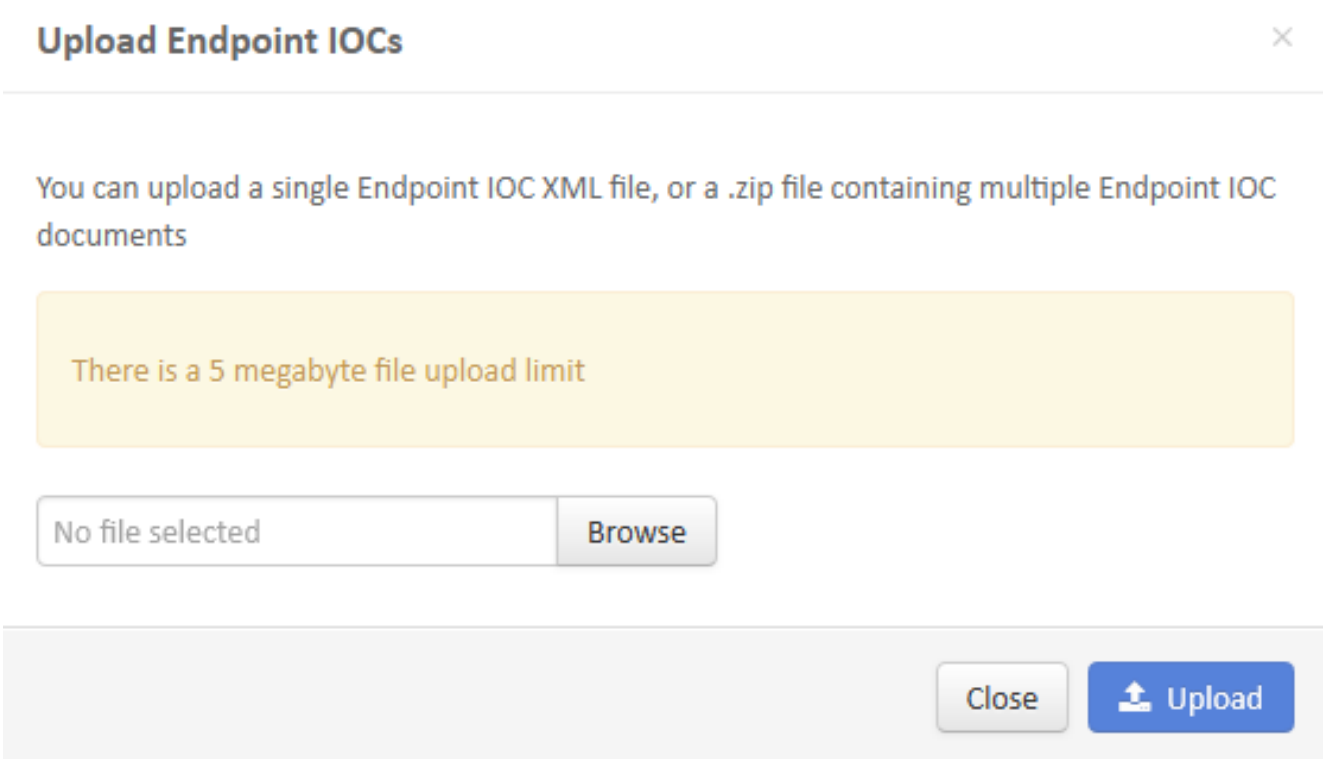
スキャンを行うために、FireAMP ダッシュボードに IOC ファイルをアップロードして下さい。 複数の IOC ファイルが含まれている IOC 署名 ファイル、XML ファイルを、または zip アーカイブを使用できます。 ダッシュボードは IOC シグニチャとのファイルを復元し、解析します。 不適切な構文かサポートされていないプロパティが使用される場合知らせられます。

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。

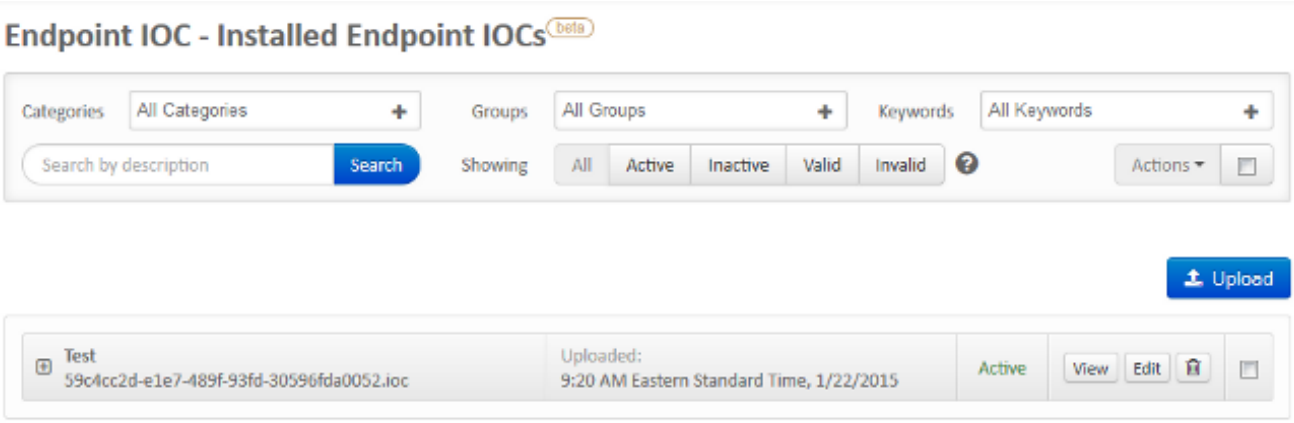
FireAMP ダッシュボードに IOC 署名 ファイルをアップロードするためにこれらのステップを完了して下さい:

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。

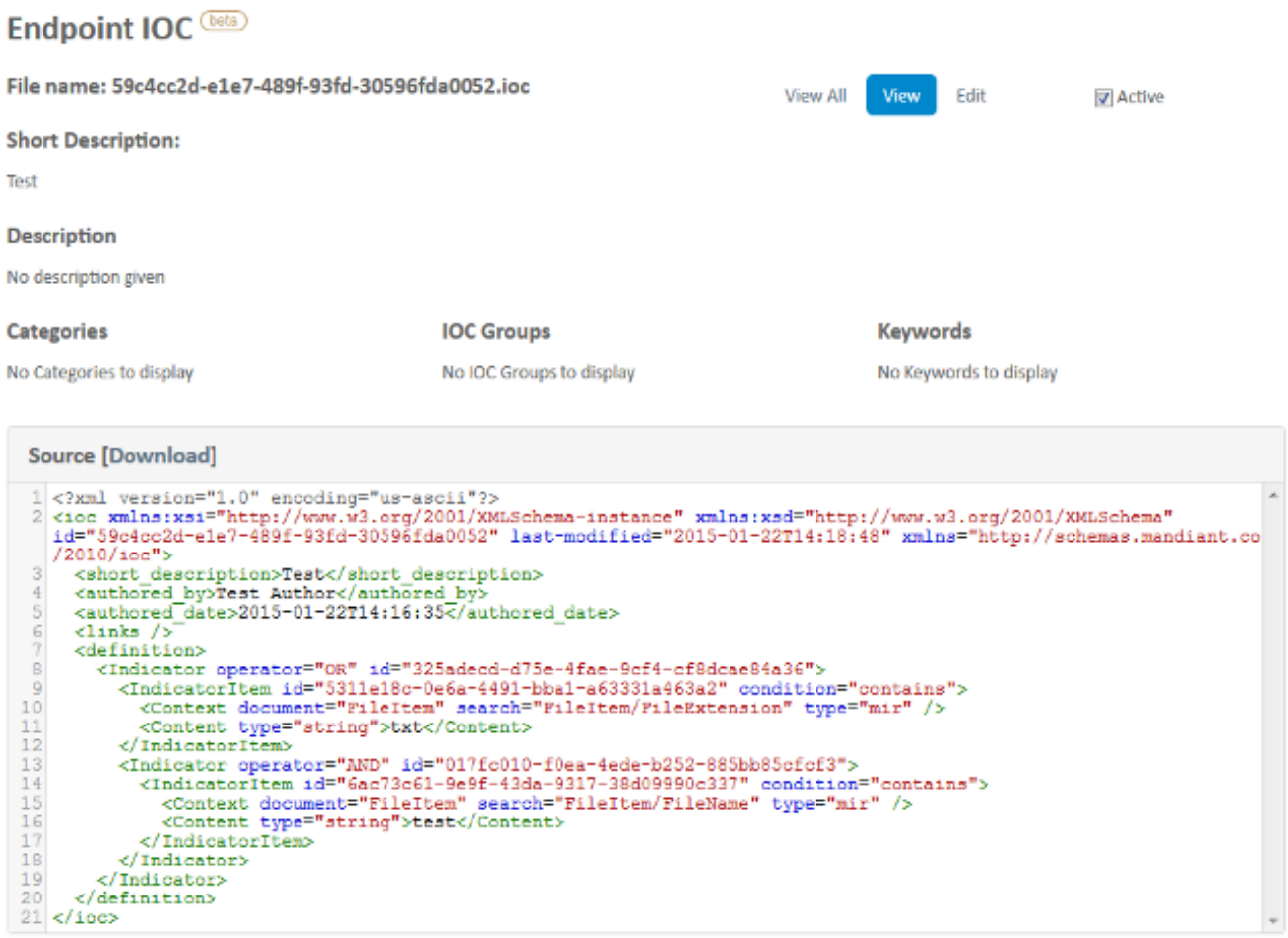
2. 『Upload』 をクリック すれば、**アップロード エンドポイント IOC** ウィンドウは現われます:



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:



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:



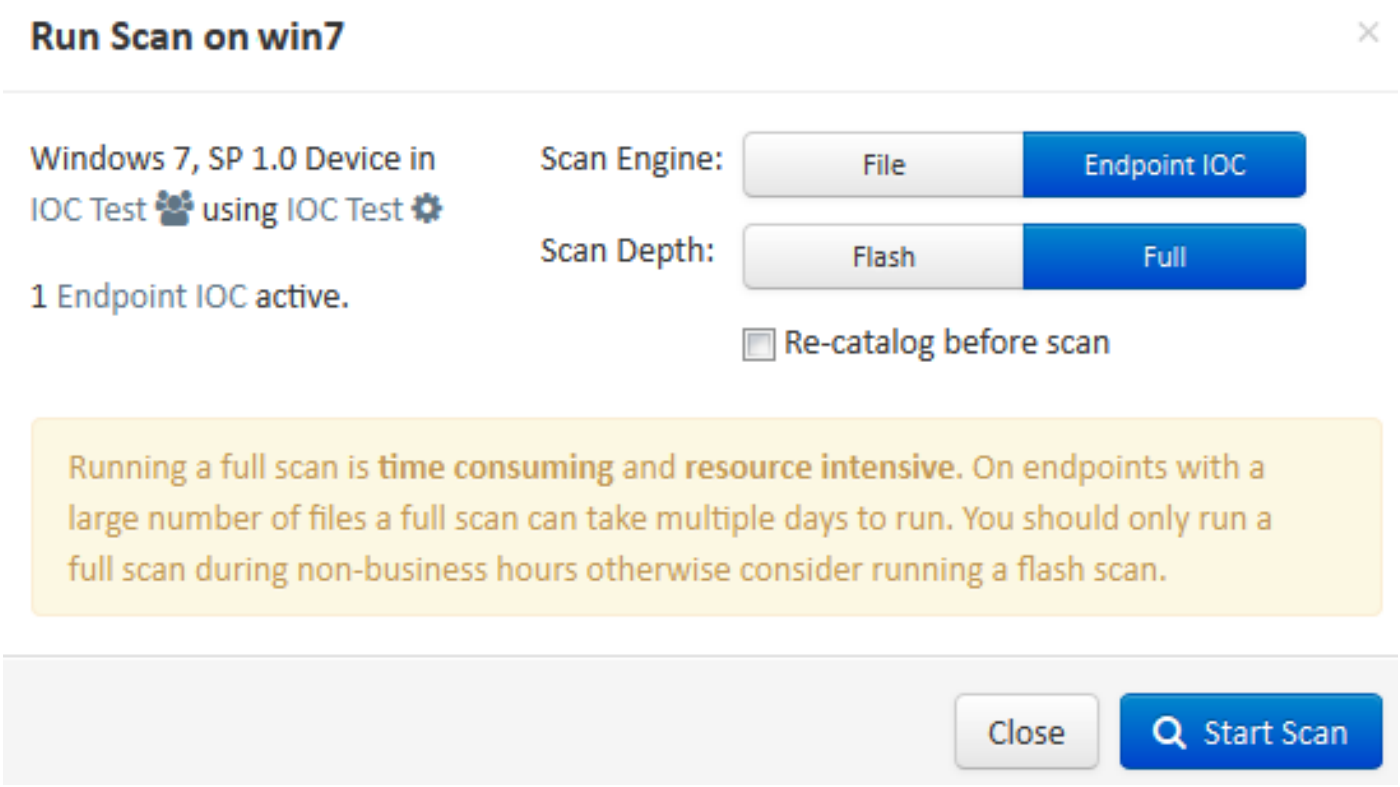
スキャンを始めて下さい

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ので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。

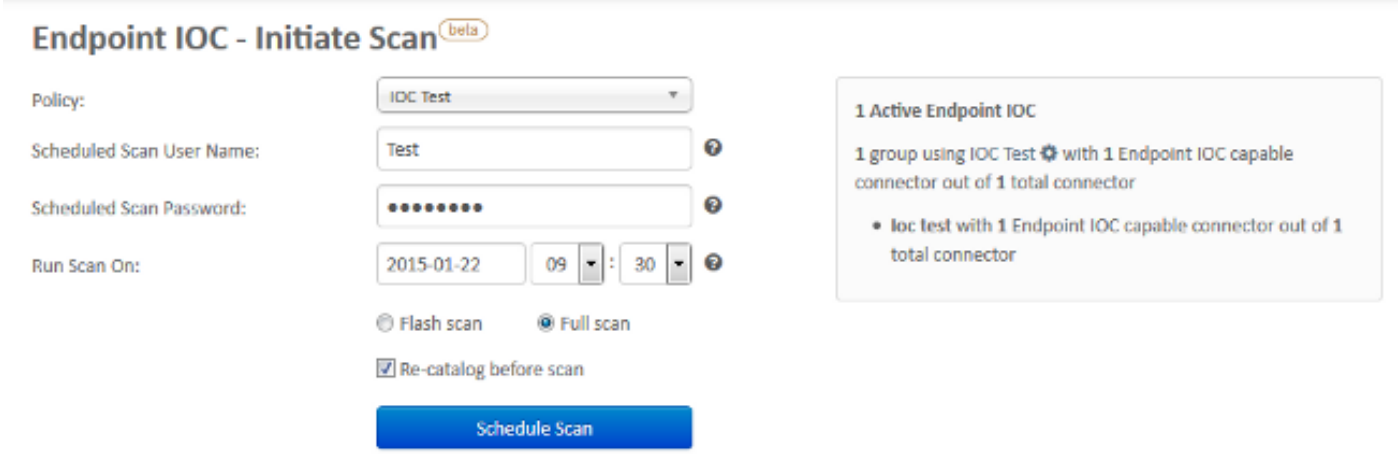
> **注:** 完全なスキャンは非常に CPU 中心です。 Cisco は使用中の間、PC の完全なスキャンをしないことを推奨します。 機能を常用するために計画する場合カタログを再製するために完全なスキャンを月に一度行うことができます。

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。

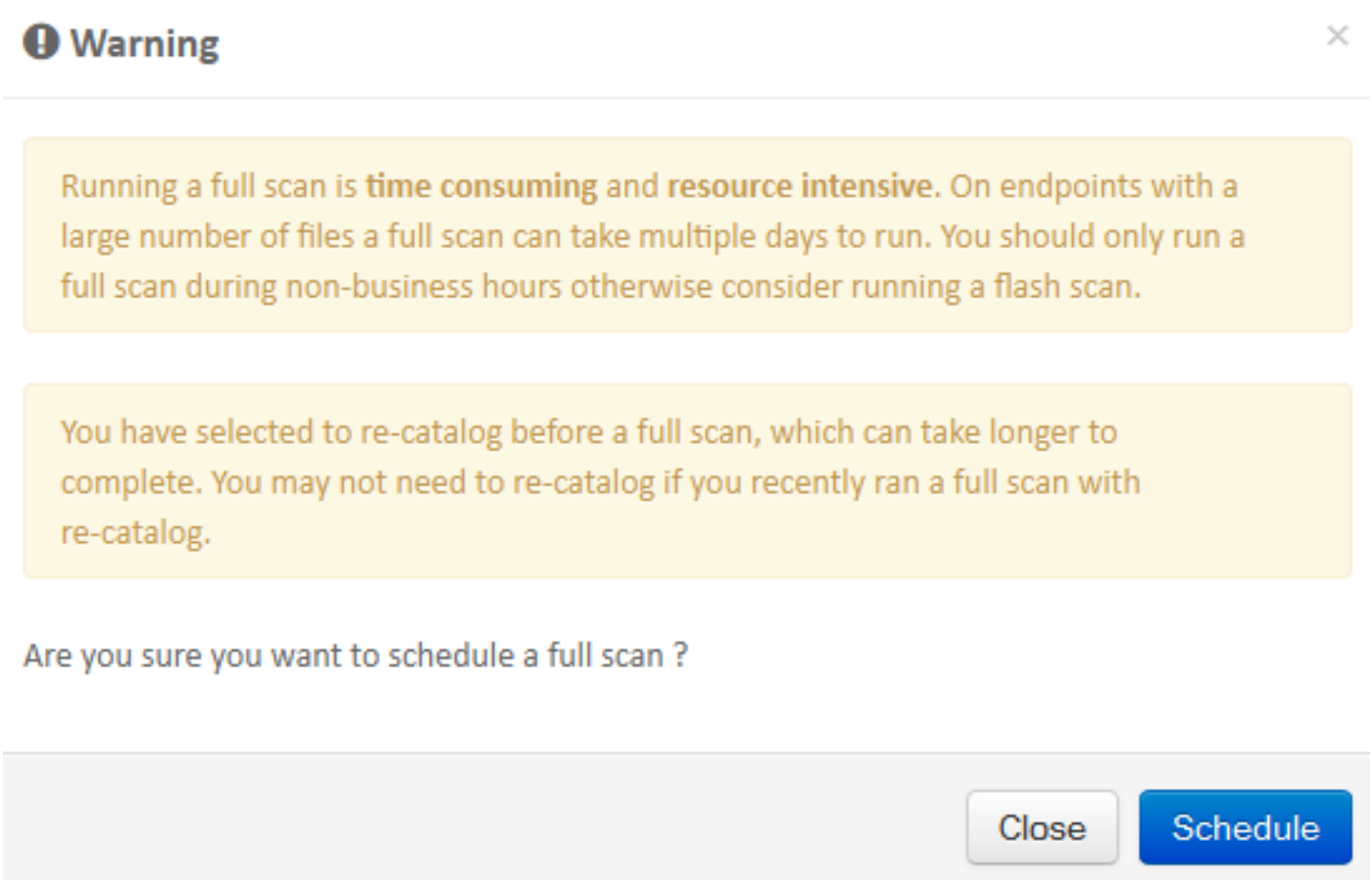
> **注:** 完全なスキャンをすることこれが最初になら、**スキャン** オプション**の前に再カタログを**チェックするために必要となりません。



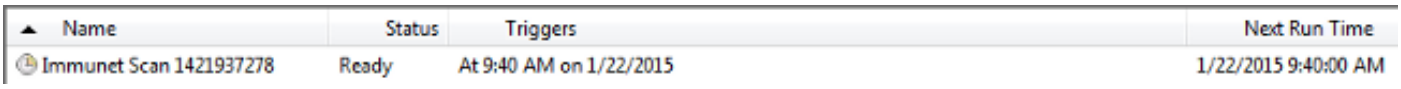
第 2 方式はダッシュボードの**発生コントロール メニュー**からのスケジュールされたエンドポイント IOC スキャンを作成することです。 このオプションはオフピーク の 時間の間にスキャンを行うことを望むとき理想的であるかもしれません。 特定のコンピューターの権限が Scheduled Tasks を作成し、**ログインをバッチ** グループ ポリシー権限**として**許可するためにあるアカウントの資格情報を提供して下さい。



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:

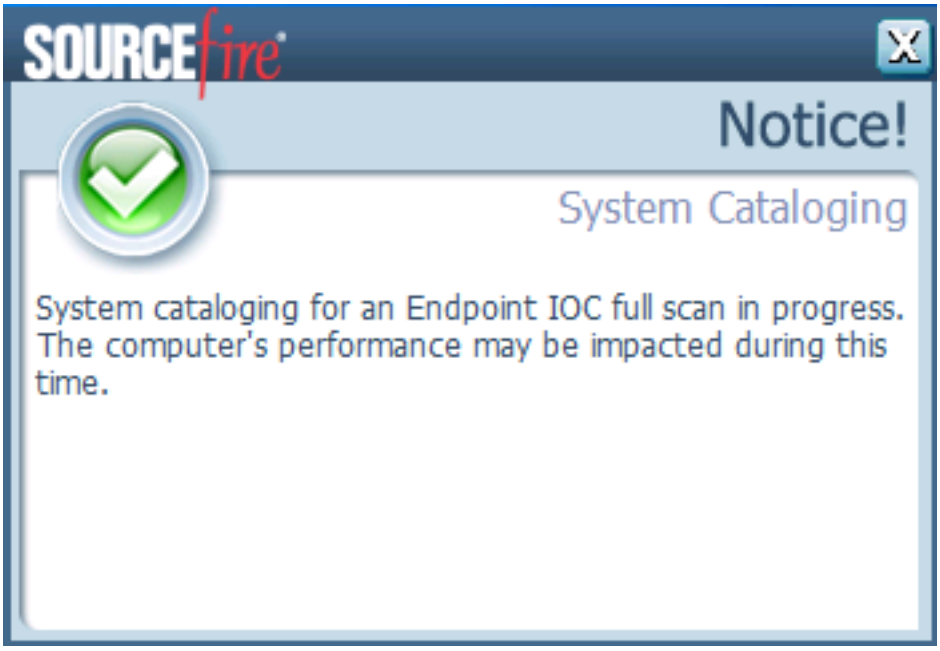


その PC がハートビートを送信 する時次に、そして資格情報が有効なら、Windows タスク スケジューラでこれと同じようなジョブを見るはずです:



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: