エンドポイント用AMPまたはFireAMPによるエンドポイントIOCスキャンの実行

内容

概要

このドキュメントでは、Mandiant IOC エディタで侵入の痕跡（IOC）署名ファイルを作成する方法、Cisco FireAMP ダッシュボードにこのファイルをアップロードする方法、およびエンドポイント IOC スキャンを開始する方法について説明します。

前提条件

要件

エンドポイント IOC スキャンを実行する前に、ドライブに 1 ギガバイト以上の空き容量があることを確認することを推奨します。

使用するコンポーネント

このドキュメントの情報は、Cisco FireAMP Windows Connector バージョン 4.0.2 以降で利用可能なエンドポイント IOC スキャナに基づいています。

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

エンドポイント IOC スキャナ機能は、複数のコンピュータにわたり、セキュリティ侵害後のインジケータをスキャンするために使用する、強力なインシデント対応ツールです。

> **注：**FireAMP では Mandiant 言語で IOC をサポートしていますが、Mandiant IOC エディタ自体はシスコにより開発されたものではなく、シスコではサポートしていません。シスコサポートでは、ユーザが作成した IOC またはサード パーティ製 IOS のトラブルシューティングは行いません。

IOC シグニチャ ファイル

IOC シグニチャ ファイルは、既知の脅威、攻撃者の攻撃手法、またはその他の侵害の証拠を特定する技術特性を説明する、拡張可能な XML スキーマです。

エンドポイント IOC は、OpenIOC ベースのファイルからコンソール経由でインポートされます。このファイルは、名前、サイズ、ハッシュなどのファイル プロパティと、プロセス情報、実行中のサービス、Microsoft Windows レジストリ エントリなどのシステム プロパティをトリガーとして使用するように作成されています。IOC 構文は、インシデント対応者が特定のアーティファクトを検索したり、マルウェア ファミリの洗練された相関検出を作成するロジックを使用したりするために使用できます。

IOC シグニチャ ファイルでのスキャンの実行

IOC シグニチャ ファイルでスキャンを実行するには、以下の 3 つのステップを完了する必要があります。

1. IOC シグニチャ ファイルを作成します。
2. IOC シグニチャ ファイルをアップロードします。
3. スキャンを開始します。

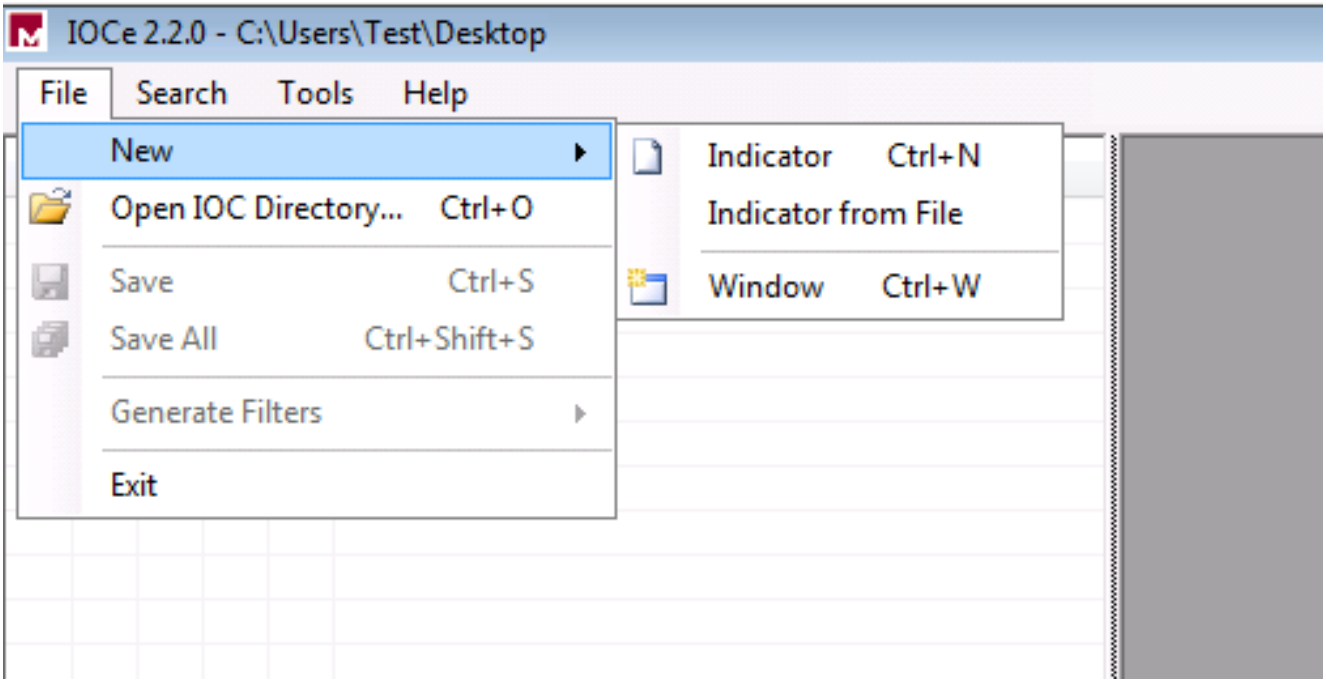
以降のセクションで、これらのステップについて説明します。

IOC シグニチャ ファイルの作成

> **注：**この例では、Mandiant IOC エディタを使用して、**test.txt** という名前のテキスト エディタの IOC シグニチャ ファイルを作成します。

IOC シグニチャ ファイルを作成するには、次の手順を実行します。

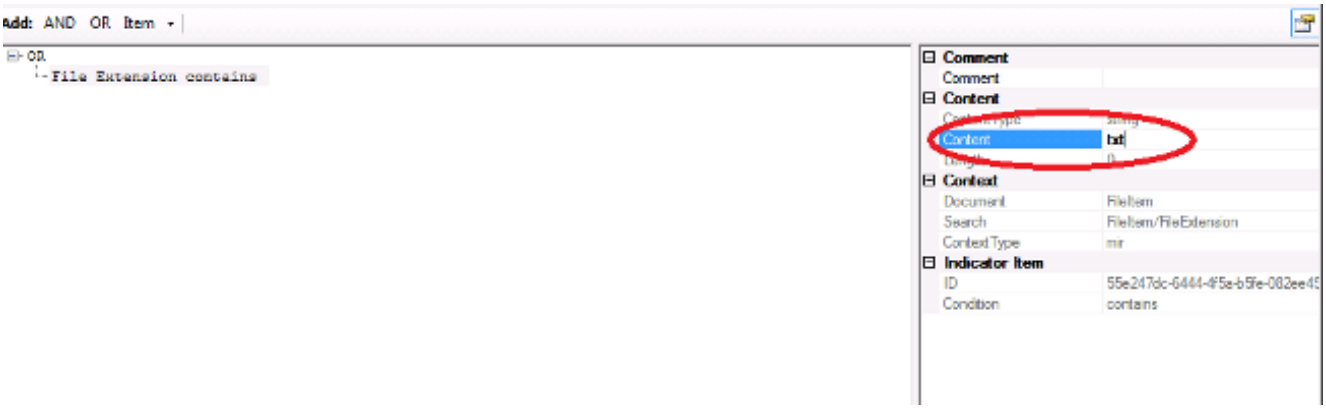
1. [IOCe]を開き、[File] > [New] > [Indicator] に移動します。ブランクのワークスペースが表示されます。ここで、IOC の作成を開始できます。



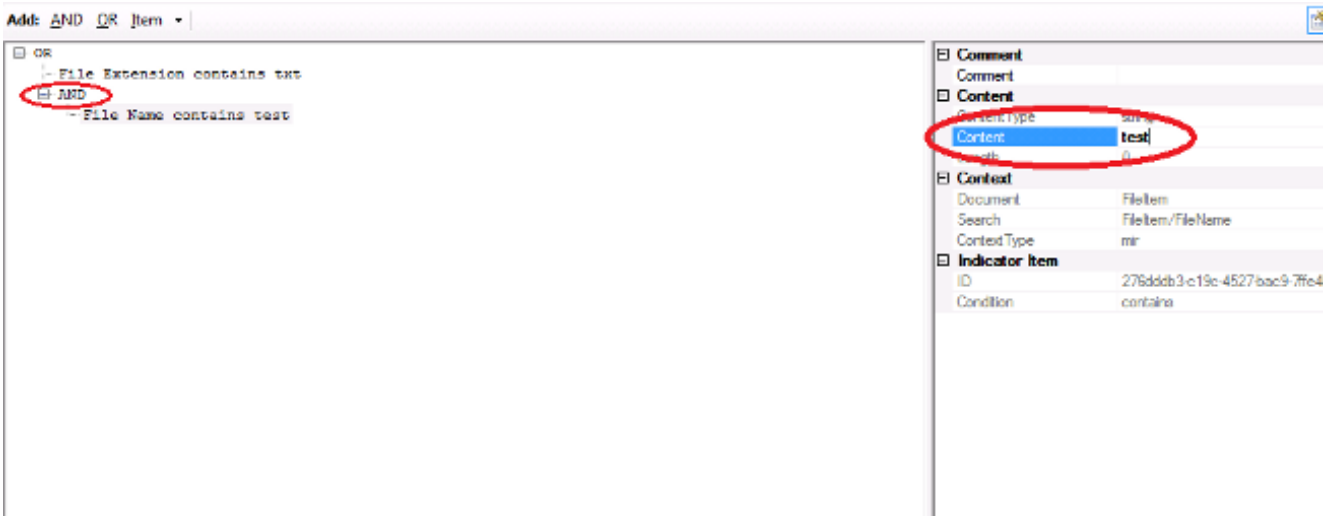
注：特定の目的に応じた IOS を作成する場合は、該当するプロパティを備えたバイナリ ロジックを使用します。初期演算子は OR です。この最も単純な演算子をベースに、作業を開始できます。これにより IOC の初期機能が有効になるので、演算子を変更する必要はありません。スキャンで IOS シグニチャ ファイルを使用するには、少なくとも 2 つのプロパティまたは条件がファイルに設定されている必要があります。

2. 演算子を追加するために、[Items]ドロップダウン メニューをクリックします。追加する必要がある最初のプロパティは、[File Extension contains]です。[Items]ツリー メニュー内でこのプロパティを見つけてクリックします。

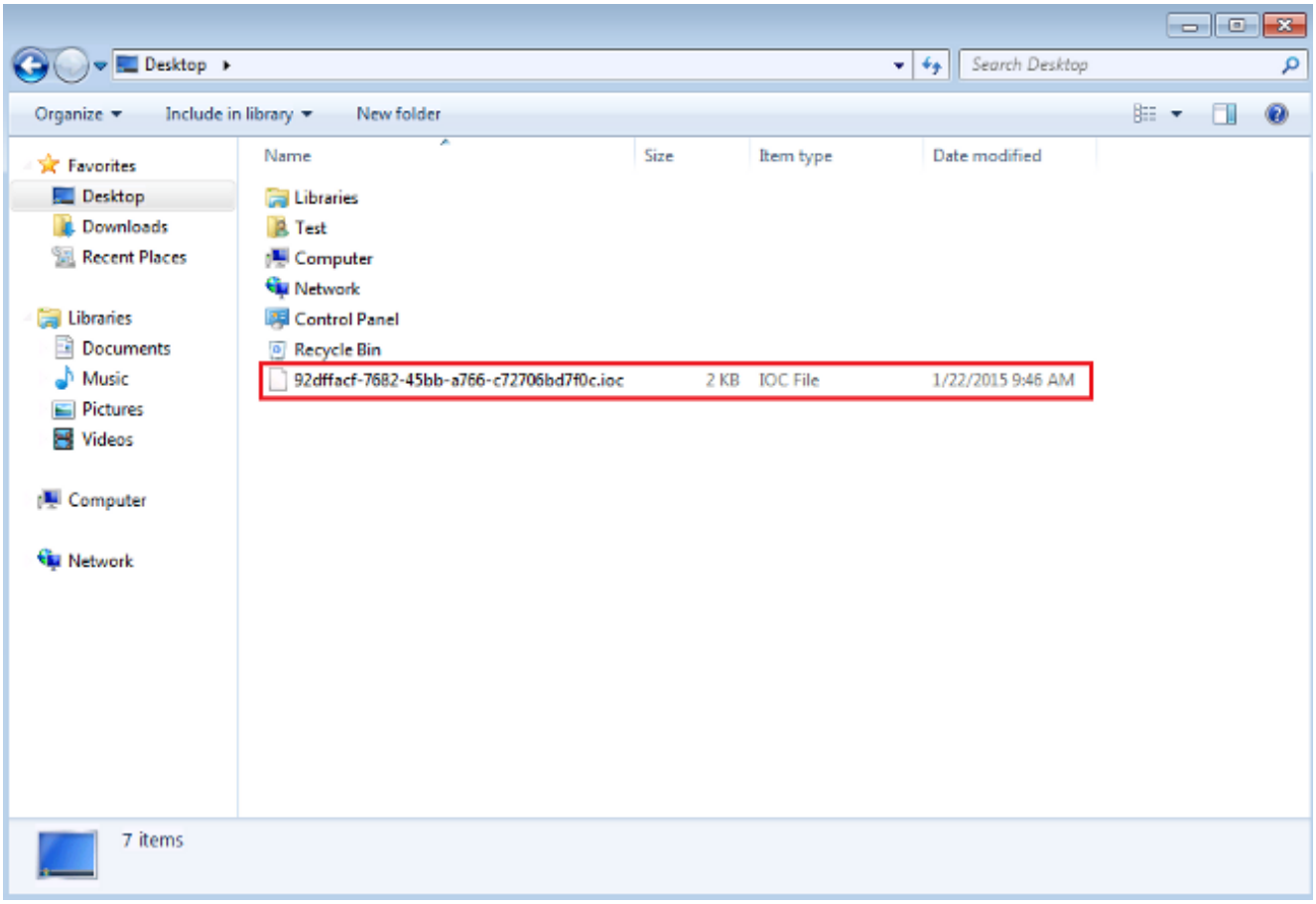
3. プロパティを追加した後、画面右端にある小さいアイコンをクリックして [Configuration] ペインを開きます。このペイン内の [Content]フィールドを使用して、照合するファイル拡張子を追加します。たとえば、**test.txt ファイルを照合するには、[txt] を追加します。**



4. 次は、論理演算子を追加する必要があります。この例では、[test]テキスト ファイルと一致させるので、[AND]演算子を使用して、次のプロパティを追加します。[Items]ツリー メニュー内でファイル名を見つけて選択します。[Properties] ペインで、検索対象のファイルの名前を追加します。たとえば、[Content] フィールドに [test]を追加します。



5. この単純な IOC には、他に追加しなければならないプロパティはないので、この時点でファイルを保存できます。[File] > [Save]の順にクリックします。これで、**.ioc 拡張子が付いたシグニチャ ファイルがシステムに保存されます。**



IOC シグニチャ ファイルのアップロード

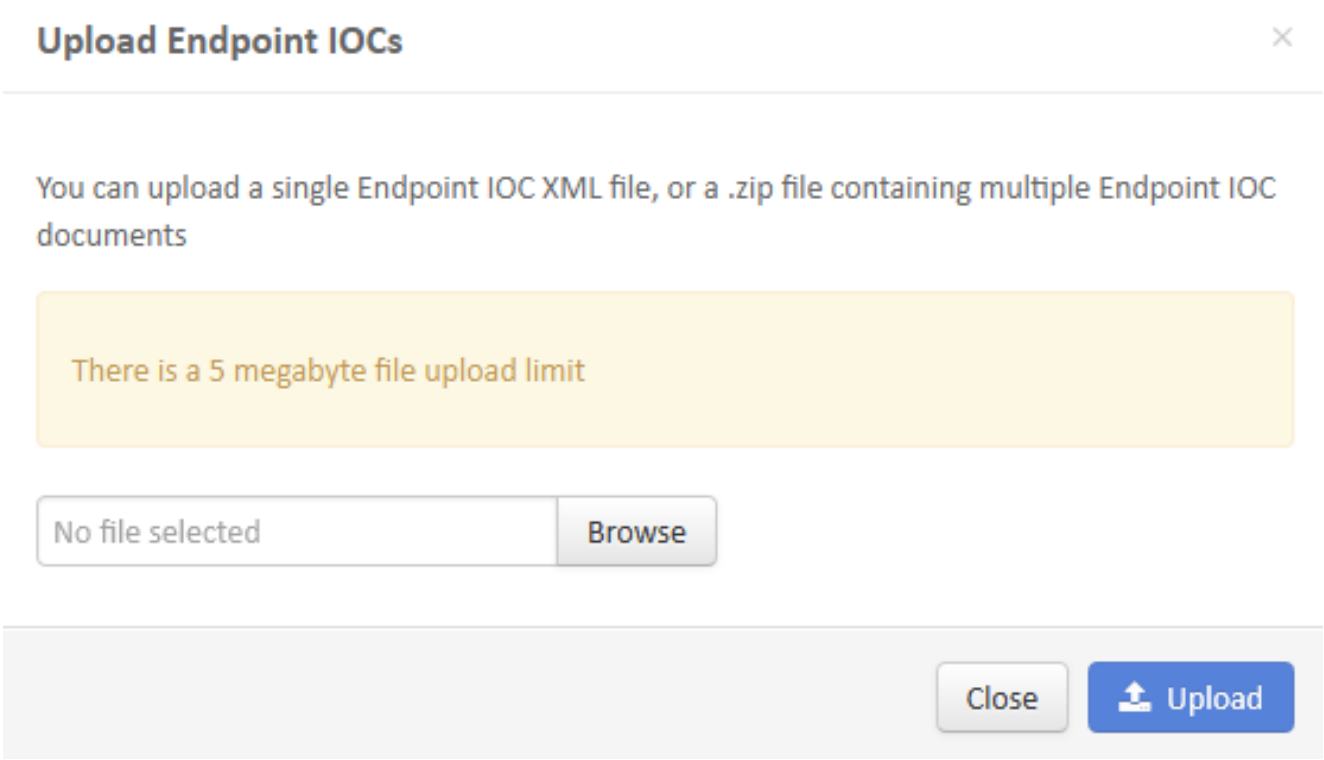
スキャンを実行するには、IOC ファイルを FireAMP ダッシュボードにアップロードする必要があります。IOC シグニチャ ファイル、XML ファイル、あるいは複数の IOC ファイルが含まれる zip アーカイブを使用できます。ダッシュボードによって圧縮解除されて、IOC シグニチャを含むファイルが解析されます。構文エラーがある場合や、サポートされていないプロパティが使用されている場合は、通知されます。

ヒント：アップロードできるファイルのサイズは、最大 5 メガバイトです。

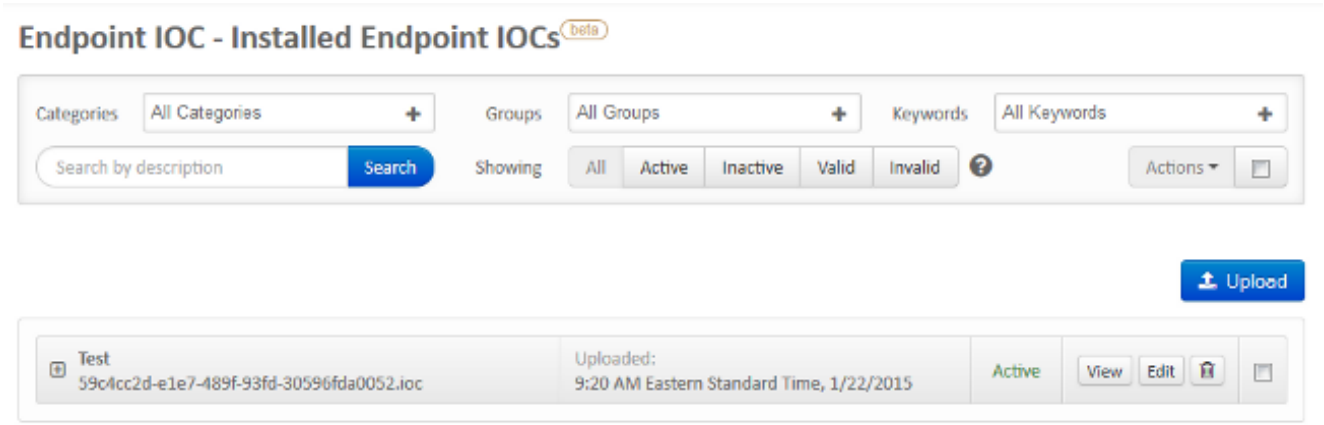
以下の手順に従って、IOC シグニチャ ファイルを FireAMP ダッシュボードにアップロードします。

1. FireAMP クラウド コンソールにログインし、[Outbreak Control] > [Installed Endpoint IOC]に移動します。

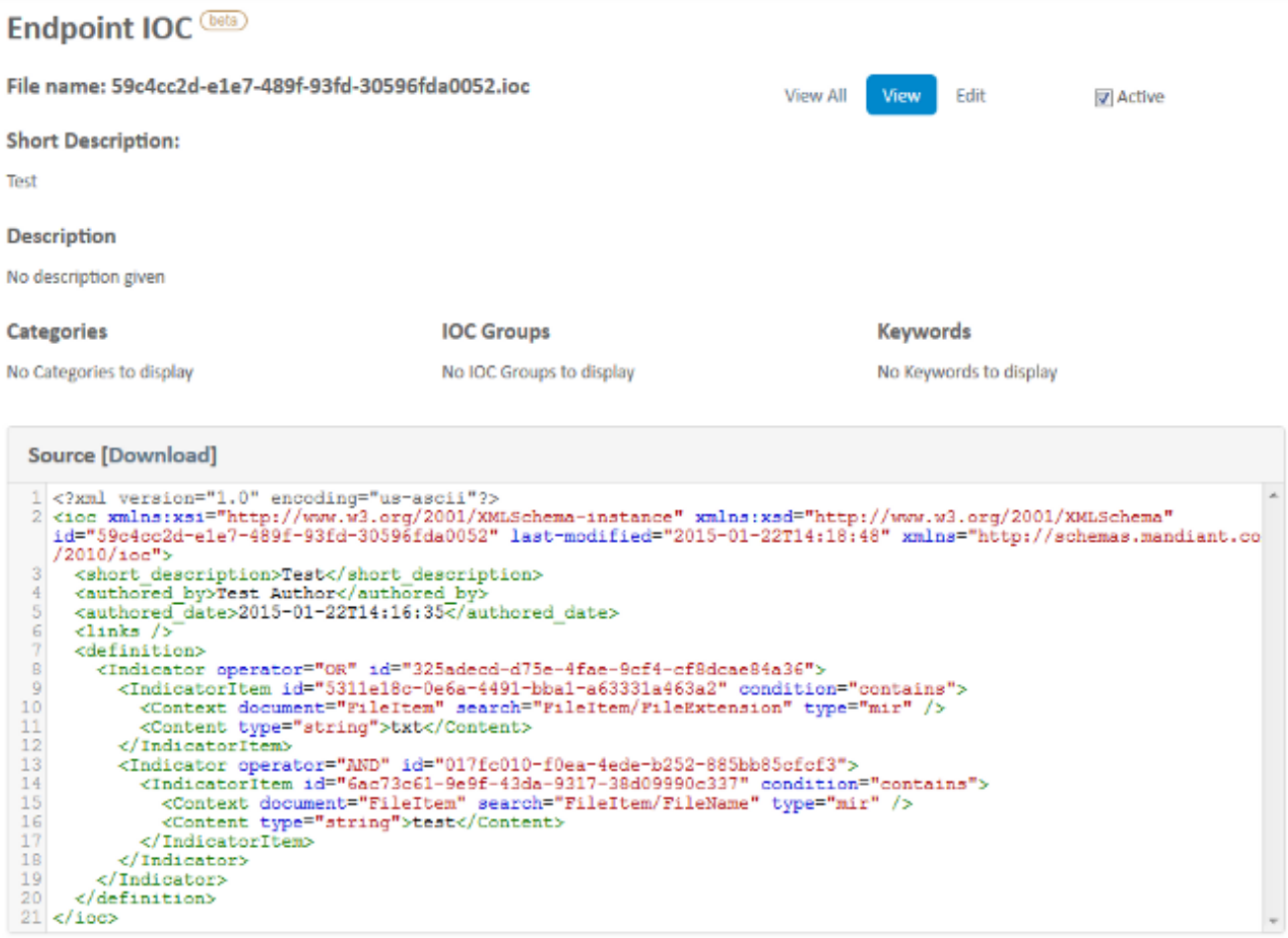
2. [Upload]をクリックします。これにより、[Upload Endpoint IOCs] **ウィンドウが表示されます。**



IOC シグニチャ ファイルのアップロードが正常に完了すると、シグニチャがリストに表示されます。



3. シグニチャの実際の XML データを表示するには、[View]をクリックします。



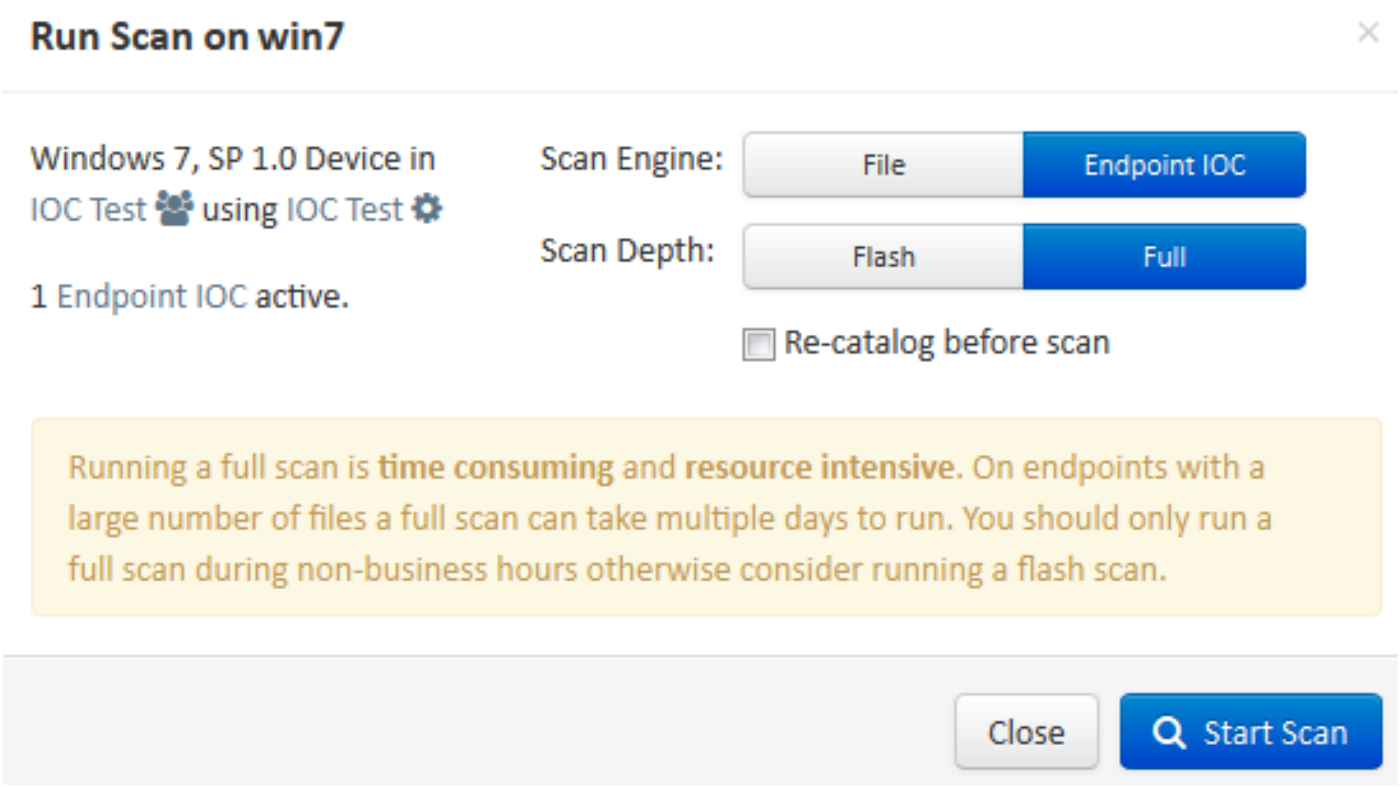
スキャンの開始

シグニチャ ファイルをアップロードした後、*フル スキャンを実行します*。最初のスキャンは、コンピュータ全体のメタデータのカタログを作成する必要があるため、フルスキャンである必要があります。これは、1 ~ 2時間かかる可能性があります。フル スキャンによってシステムのカタログが構築された後は、*フラッシュ スキャンを実行できます*。

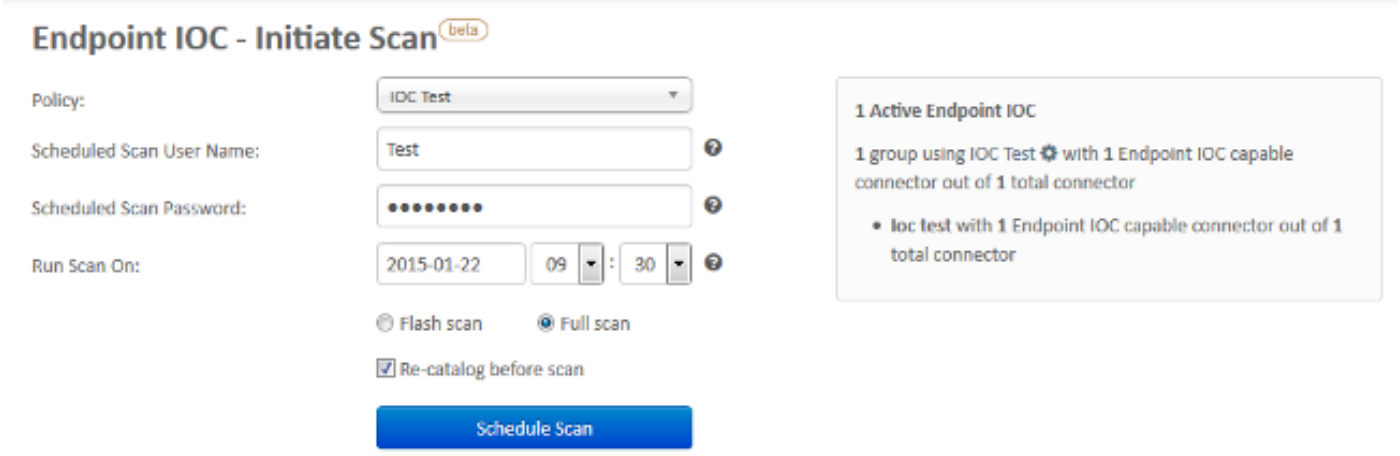
> **注**：フル スキャンは CPU を駆使します。PC の使用中にはフル スキャンを実行しないようにしてください。このスキャン機能を定期的に使用する予定の場合は、カタログを再構築するために毎月 1 回フル スキャンを実行できます。

IOC スキャンを実行するには、2 つの方法を使用できます。1 つは、イベントまたはダッシュボードから即時スキャンを実行するという方法です。このスキャンは、次回 PC がクラウドにハートビートを送信するとトリガーされます。

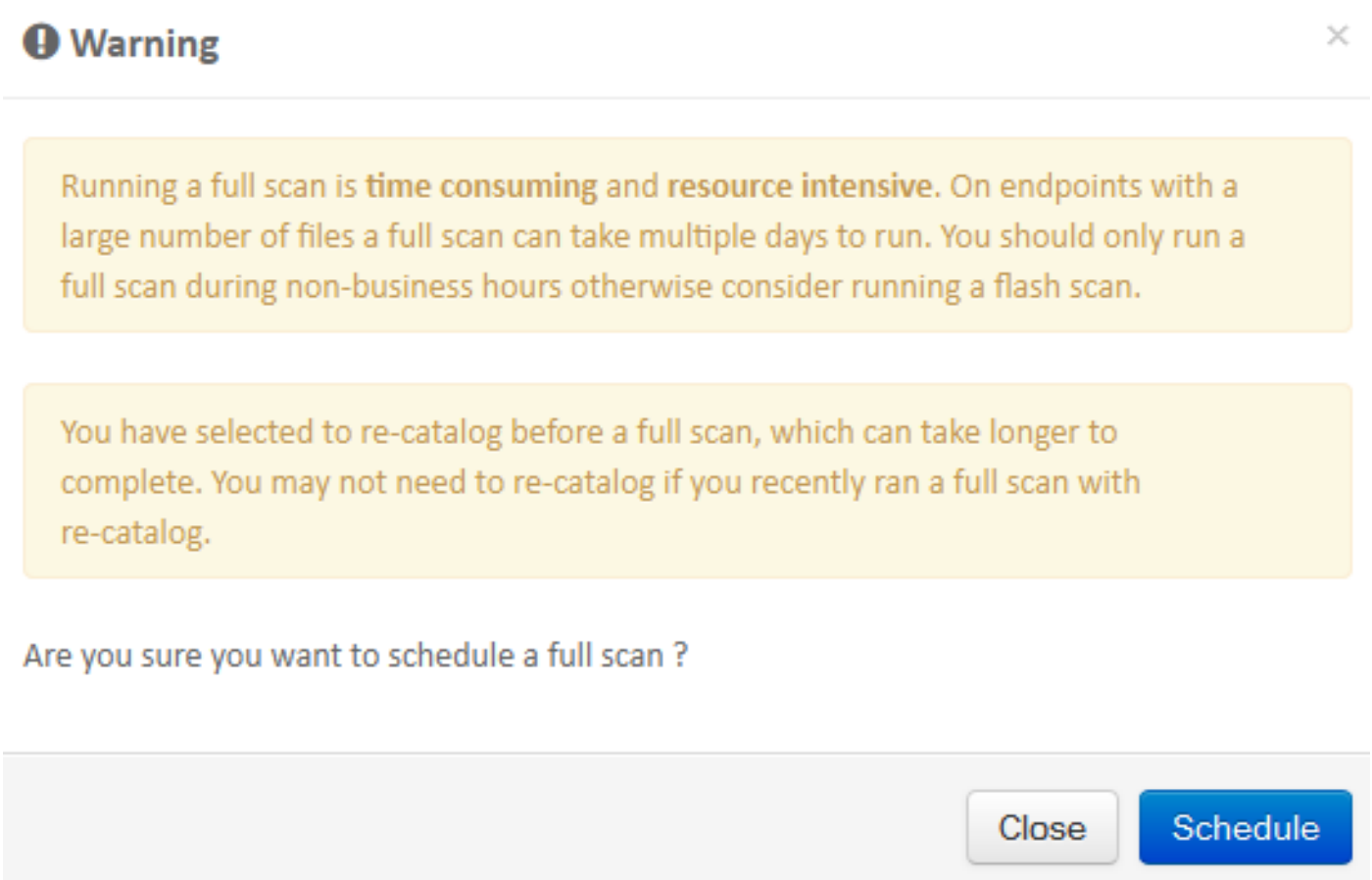
> **注**：初めてフル スキャンを実行する場合は、[Re-catalog before scan]オプションをオンにする必要はありません。



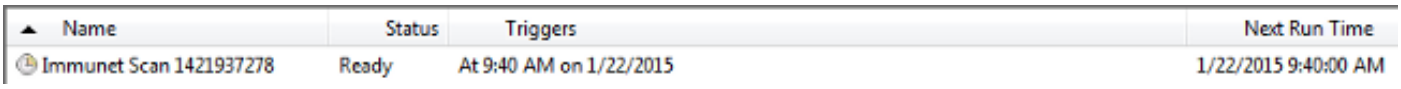
もう 1 つの方法は、ダッシュボードの [Outbreak Control]メニューから、スケジュールされたエンドポイント IOC スキャンを作成することです。オフピーク中にスキャンを実行したい場合は、このオプションが最適です。スケジュールされたタスクを作成し、[Log on as Batch] グループ ポリシー アクセス権限を許可するには、対象のコンピュータへのアクセス権限が割り当てられたアカウントのクレデンシャルを入力する必要があります。



エンドポイント IOC スキャンをスケジュールする際に、以下の警告メッセージが表示されます。

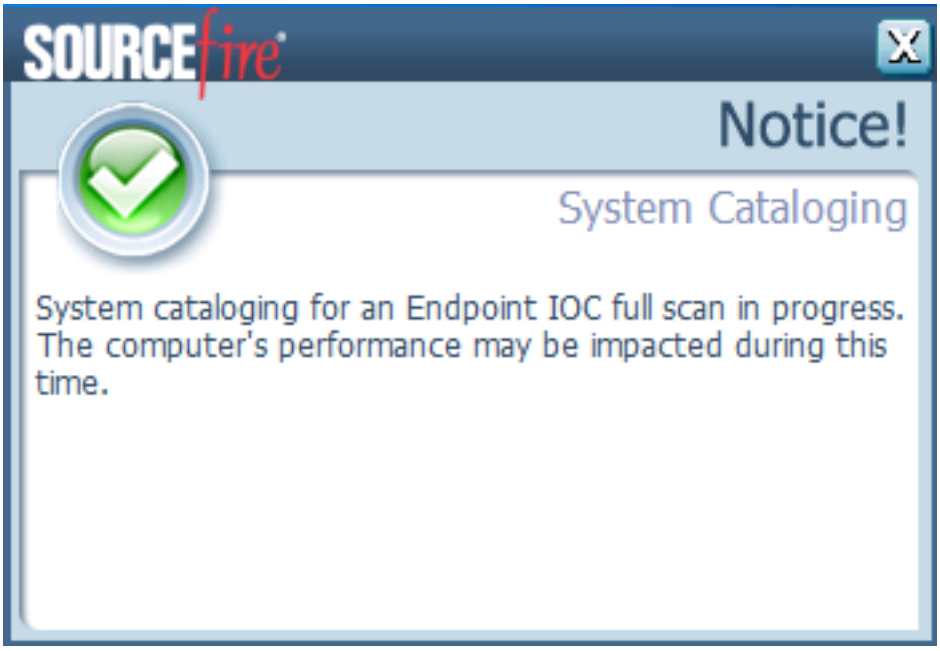


入力したクレデンシャルが有効であれば、次回 PC がハートビートを送信するときに以下のようなジョブが Windows タスク スケジューラに表示されます。



スキャンが開始すると、以下のメッセージが表示されます。

注：非表示になるように GUI が設定されている場合、[System Cataloging]メッセージは表示されません。



スキャンが完了した後、[Endpoint IOC Scan Detection Summary]を表示できます。以下の例に、**test.txt IOC シグニチャ ファイルの一致結果を示します。**