Execute a indicação do valor-limite de varreduras do acordo (IOC) com o ampère para valores-limite ou FireAMP

Índice

Introdução

Este documento descreve como criar uma indicação do arquivo de assinatura do acordo (IOC) através do editor de Mandiant IOC, como transferi-lo arquivos pela rede ao painel de Cisco FireAMP, e como iniciar uma varredura do valor-limite IOC.

Pré-requisitos

Requisitos

Cisco recomenda que você tem pelo menos uma giga byte do espaço livre da movimentação antes que você tente executar as varreduras do valor-limite IOC.

Componentes Utilizados

A informação neste documento é baseada no varredor do valor-limite IOC, que está disponível nas versões 4.0.2 e mais recente do conector de Cisco FireAMP Windows.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto

potencial de qualquer comando.

Informações de Apoio

A característica do varredor do valor-limite IOC é uma ferramenta poderosa da resposta ao incidente que seja usada a fim fazer a varredura de indicadores do cargo-acordo através dos computadores múltiplos.

> Nota: Embora FireAMP apoie IOC com a língua de Mandiant, o software próprio do editor de Mandiant IOC não é desenvolvido nem é apoiado por Cisco. Cisco apoia não pesquisa defeitos IOC USER-criados ou da terceira.

Arquivos de assinatura IOC

O arquivo de assinatura IOC é um esquema elástico XML para a descrição das características técnicas que identificam uma ameaça conhecida, uma metodologia do atacante, ou a outra evidência do acordo.

Você pode importar o valor-limite IOC através do console dos arquivos OpenIOC-baseados que são redigidos a fim provocar em propriedades de arquivo tais como o nome, o tamanho, e a mistura, assim como os outros atributos e propriedades do sistema tais como a informação de processo, serviços running, e entradas de registro de Microsoft Windows. A sintaxe IOC pode ser usada por que respondes do incidente a fim encontrar produtos manufaturados específicos ou a fim usar a lógica para criar detecções sofisticadas, correlacionadas para famílias do malware.

Execute uma varredura em um arquivo de assinatura IOC

Há três etapas que você deve terminar a fim executar uma varredura em um arquivo de assinatura IOC:

1. Crie um arquivo de assinatura IOC.
2. Transfira arquivos pela rede o arquivo de assinatura IOC.
3. Inicie uma varredura.

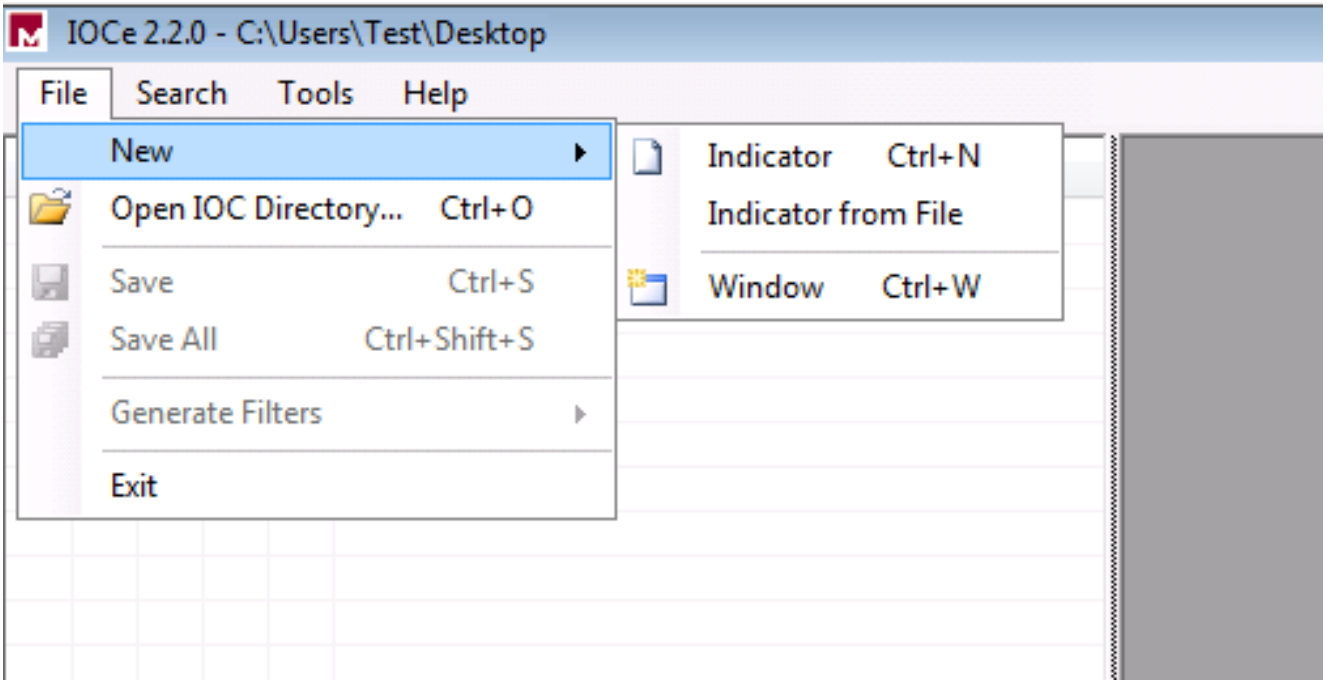
Estas etapas são expandidas em cima nas seções que seguem.

Crie um arquivo de assinatura IOC

> Nota: Neste exemplo, o editor de Mandiant IOC é usado a fim construir um arquivo de assinatura IOC para um arquivo de texto nomeado **test.txt**.

Termine estas etapas a fim criar um arquivo de assinatura IOC:

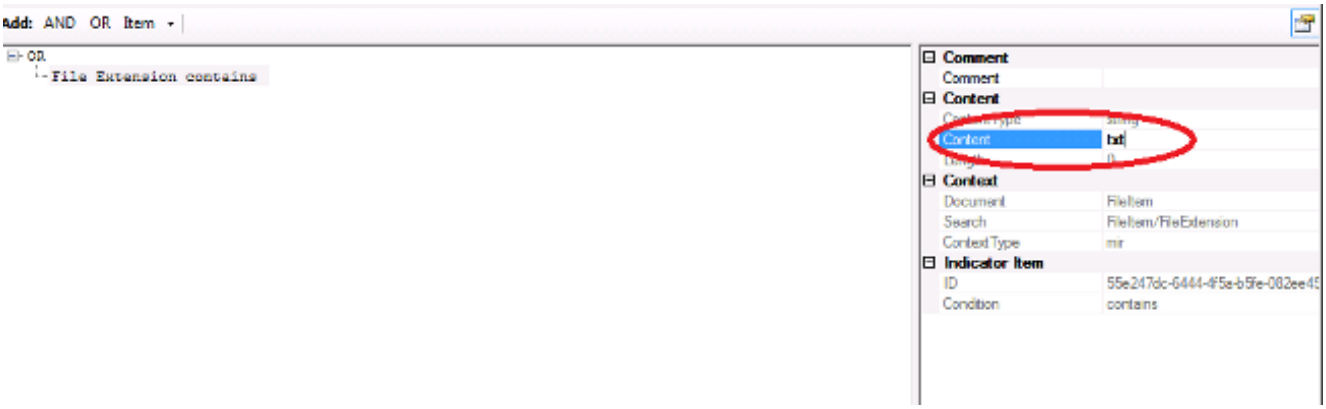
1. Abra o **IOCe** e navegue **para arquivar > novo > indicador**. Isto fornece um espaço de trabalho vazio de modo que você possa começar a construir um IOC.



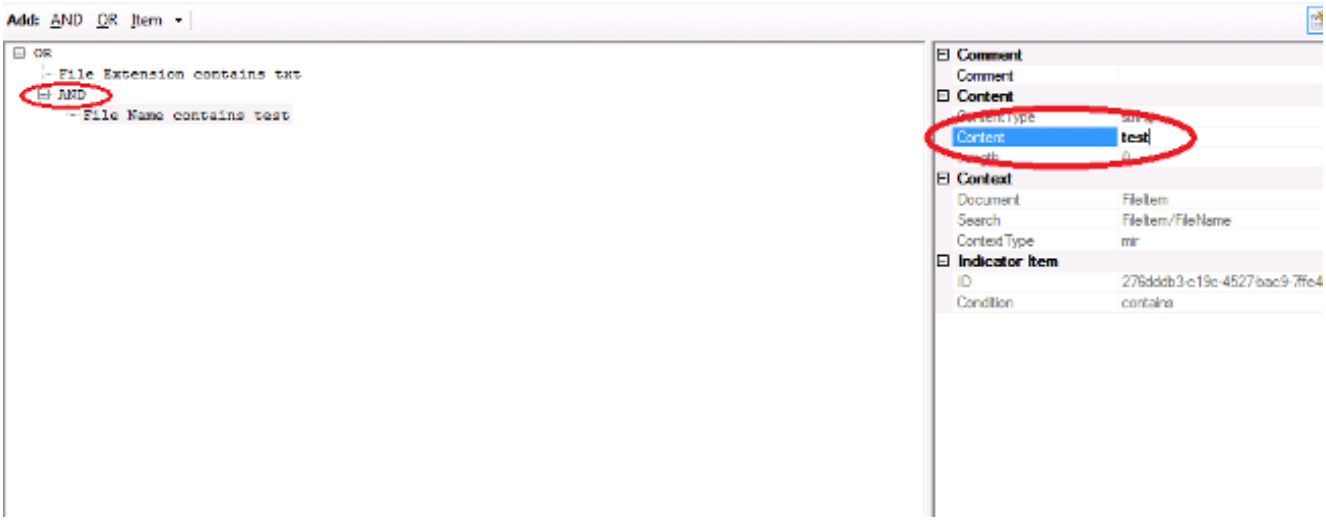
Nota: A fim criar um IOC para algo específico, use a lógica binária com as propriedades. O operador inicial é OU, de que é a base a mais simples a trabalhar. Isto permite que a função inicial do IOC trabalhe, assim que você não é exigido mudá-lo. Exige-se que um arquivo de assinatura IOC tem pelo menos duas propriedades ou circunstâncias a fim o usar com sucesso em uma varredura.

2. Clique o menu suspenso dos **artigos** a fim adicionar operadores. A primeira propriedade que você deve adicionar é **extensão de arquivo contém**. Encontre a propriedade no menu da árvore dos **artigos** e clique-a.

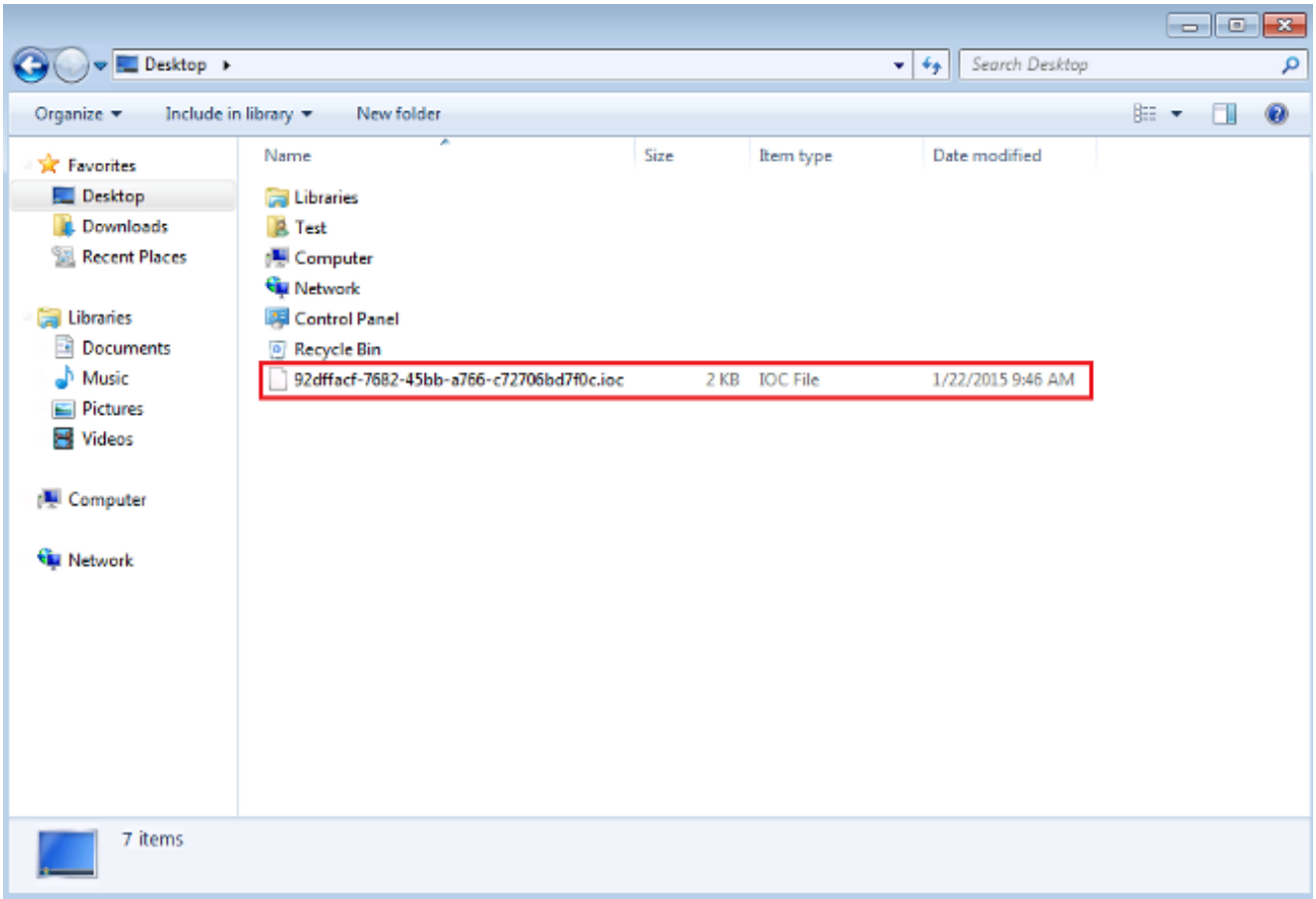
3. Depois que você adiciona uma propriedade, clique o ícone pequeno no lateral da extrema direita da tela a fim abrir a placa da configuração. Dentro desta placa, use o campo **satisfeito** a fim combinar uma extensão de arquivo. Por exemplo, adicionar o **txt** a fim combinar o arquivo de texto de **test.txt**:



4. Você deve agora adicionar um operador da lógica. Neste exemplo, você combinará o arquivo de texto do **teste**. A fim combinar isto, use *E o* operador e adicionar a propriedade seguinte. Encontre o nome de arquivo e selecione-o do menu da árvore dos **artigos**. No painel de propriedades, adicionar o nome do arquivo que você quer encontrar. Por exemplo, adicionar o **teste no** campo satisfeito:



5. Desde que nenhuma propriedade adicional é necessária para este IOC simples, você pode agora salvar o arquivo. Clique o **arquivo > salvar**, e um arquivo de assinatura com uma extensão **.ioc** salvar no sistema:



Transfira arquivos pela rede um arquivo de assinatura IOC

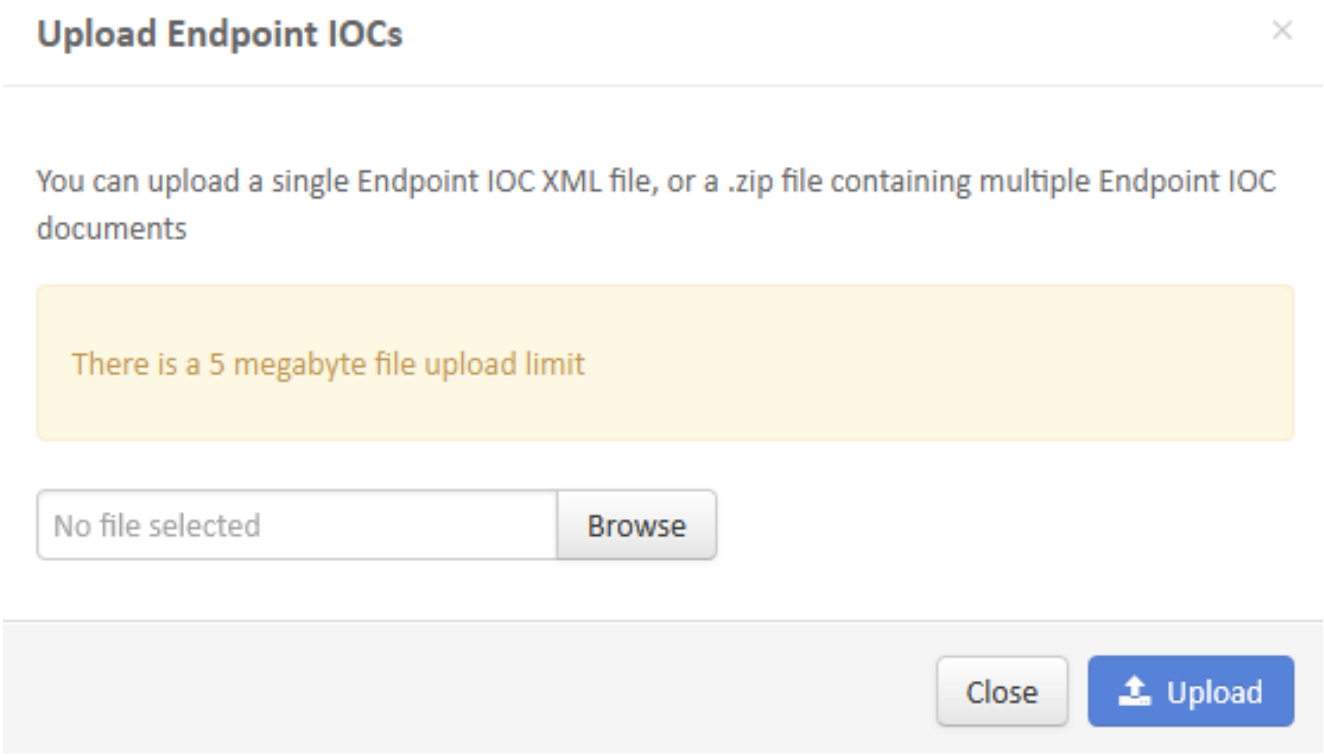
A fim executar uma varredura, você deve transferir arquivos pela rede um arquivo IOC ao painel de FireAMP. Você pode usar um arquivo de assinatura IOC, um arquivo XML, ou um arquivo do fecho de correr que contenha arquivos múltiplos IOC. O painel descomprime e analisa gramaticalmente o arquivo com as assinaturas IOC. Você é notificado se uma sintaxe incorreta ou uma propriedade unsupported são usadas.

Dica: Você pode transferir arquivos pela rede os arquivos que são até cinco megabytes em tamanho.

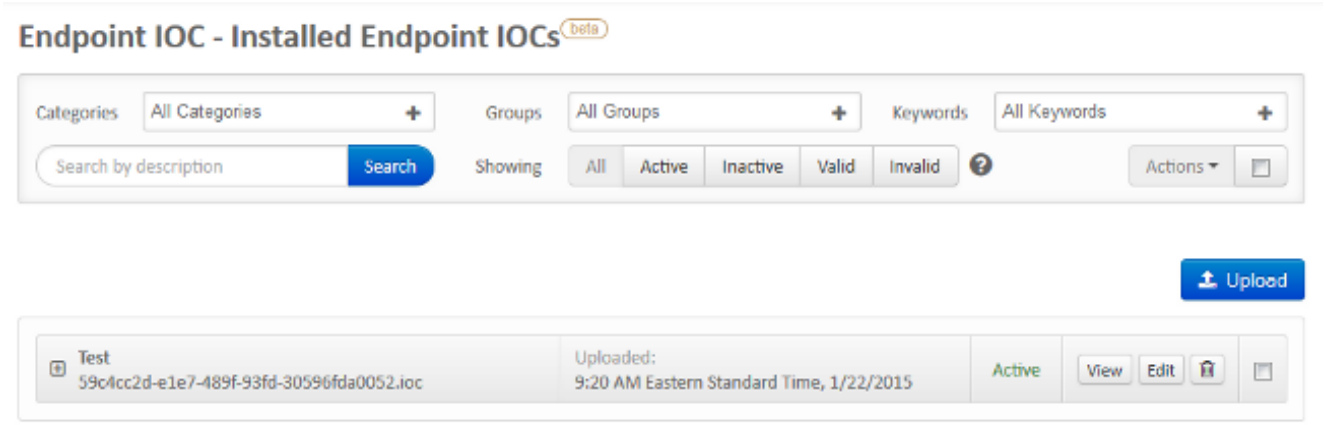
Termine estas etapas a fim transferir arquivos pela rede o arquivo de assinatura IOC ao painel de FireAMP:

1. O log no console da nuvem de FireAMP e navega ao **controle da manifestação > o valor-limite instalado IOC**.

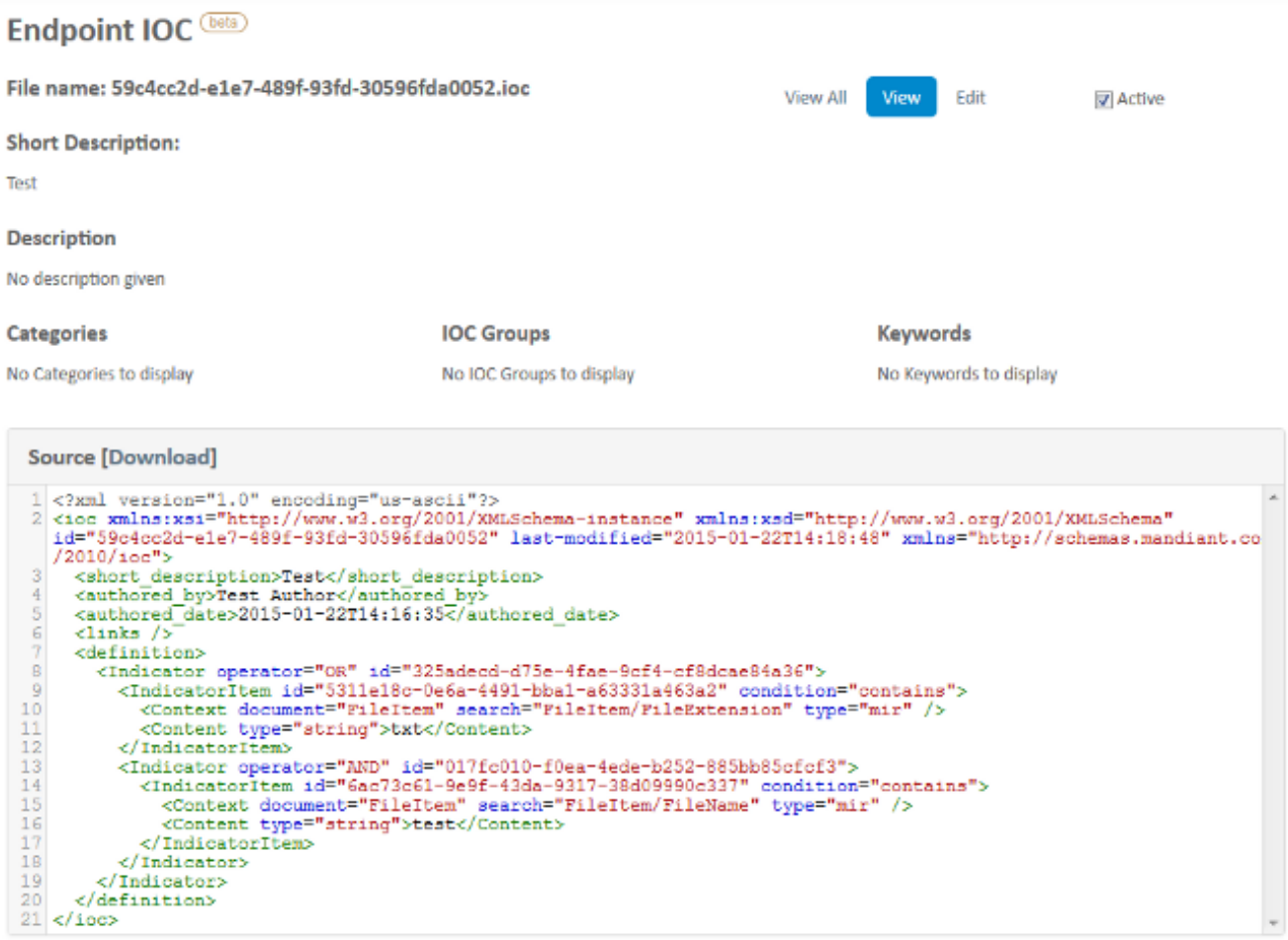
2. Clique a **transferência de arquivo pela rede**, e o indicador do **valor-limite IOC da transferência de arquivo pela rede** aparece:



Depois que um arquivo de assinatura IOC é transferido arquivos pela rede com sucesso, a assinatura aparece na lista:



3. Clique a **vista** a fim ver os dados reais XML da assinatura:



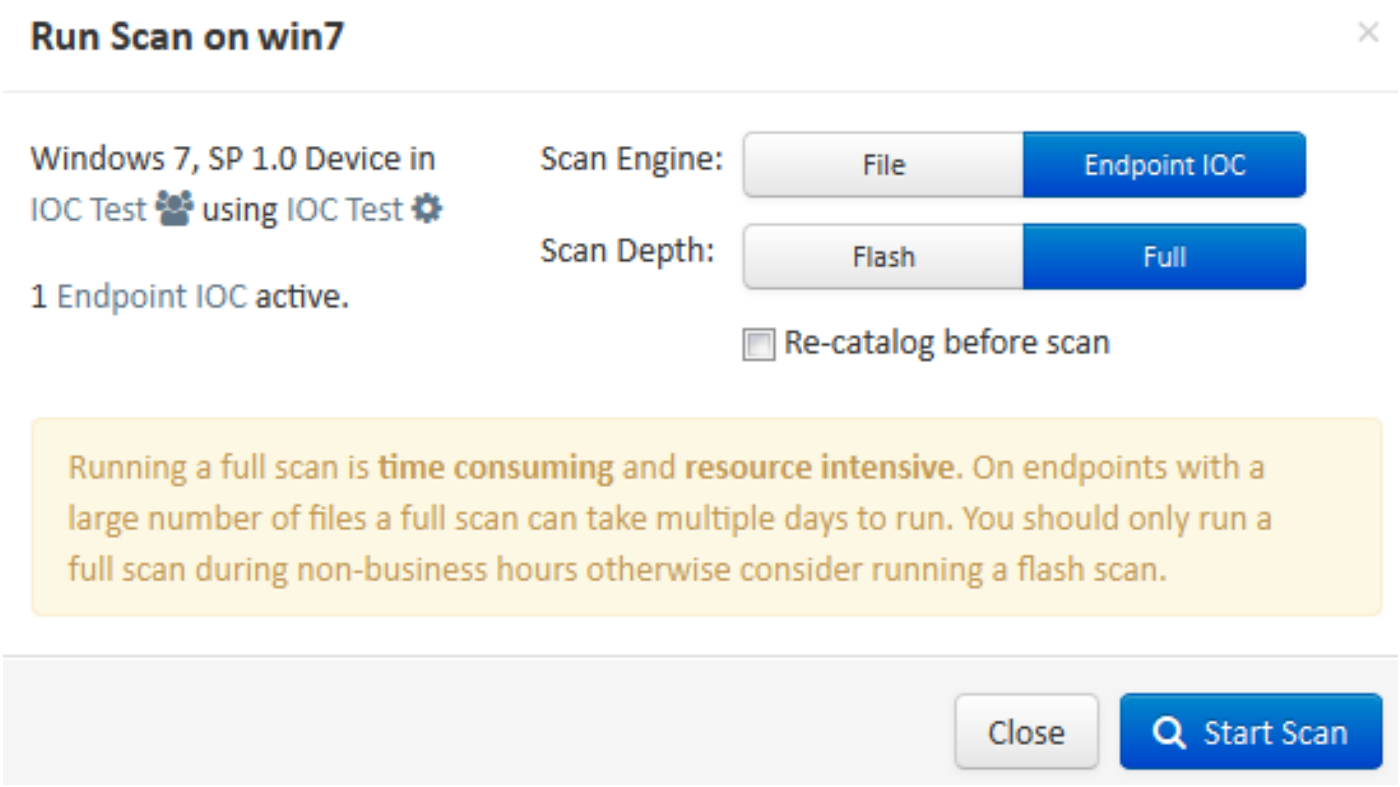
Inicie uma varredura

Depois que você transfere arquivos pela rede um arquivo de assinatura, execute uma varredura *completa*. A primeira varredura deve ser uma varredura completa porque deve construir um catálogo dos metadata para o computador inteiro, que pode tomar 1 – 2 horas. Você pode executar uma varredura *instantânea* depois que o sistema é catalogado com uma varredura completa.

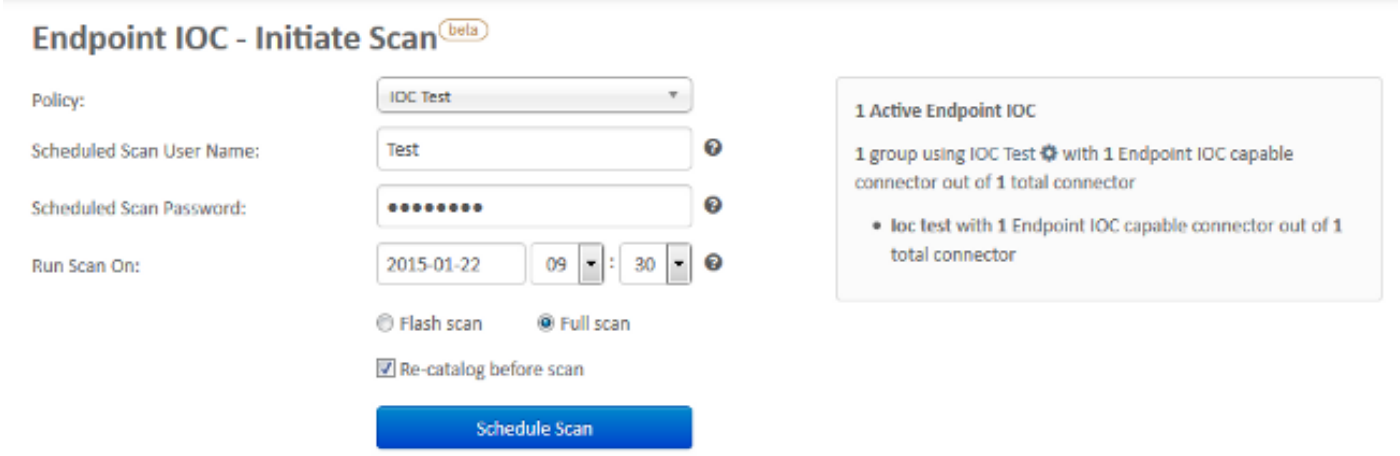
> Nota: A varredura completa é muito utilização de CPU. Cisco recomenda que você não executa uma varredura completa em um PC quando estiver no uso. Se você planeia usar regularmente a característica, você pode executar uma varredura completa uma vez por mês a fim reconstruir o catálogo.

Há dois métodos diferentes que você pode usar a fim executar uma varredura IOC. O primeiro método é executar uma varredura imediata de um evento ou do painel. Isto é provocado a próxima vez que um PC envia a uma pulsação do coração à nuvem.

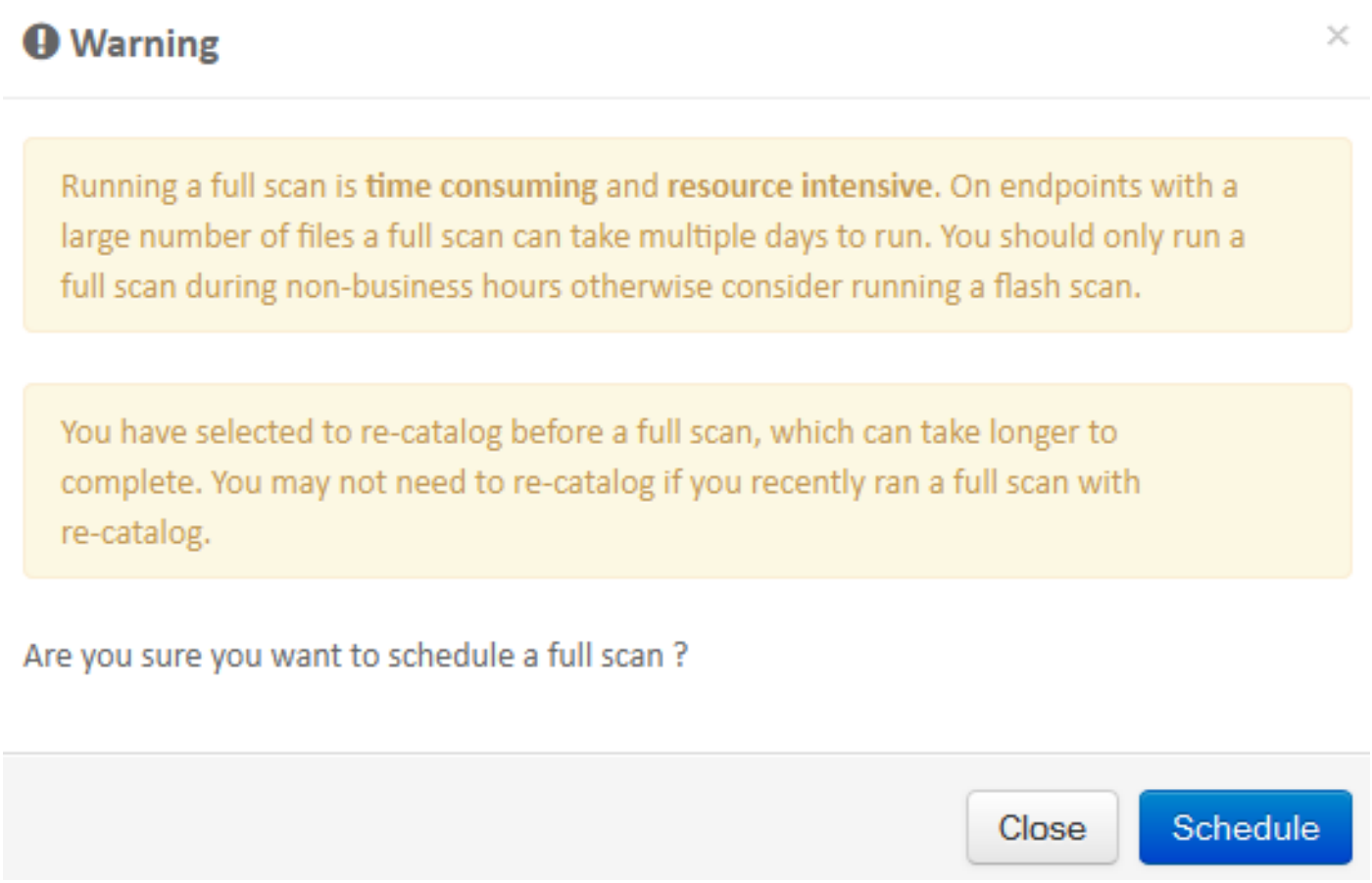
> Nota: Se isto é a primeira vez que você executa a varredura completa, você não é exigido verificar o Re-**catálogo antes da** opção da **varredura**.



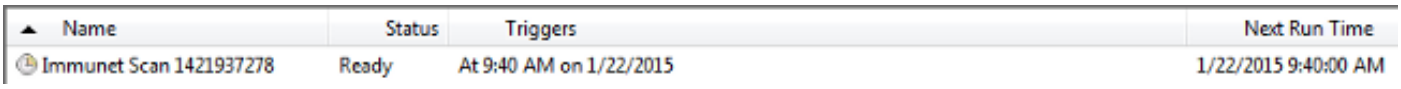
O segundo método é criar uma varredura programada do valor-limite IOC do **menu de controle da manifestação do** painel. Esta opção pôde ser ideal quando você deseja executar varreduras durante horas fora de pico. Você deve fornecer as credenciais de uma conta que tenha a permissão no computador dado a fim criar tarefas programadas e permitir o **fazer logon como a** permissão da política do grupo do **grupo**.



Quando você programa uma varredura do valor-limite IOC, este mensagem de advertência aparece:

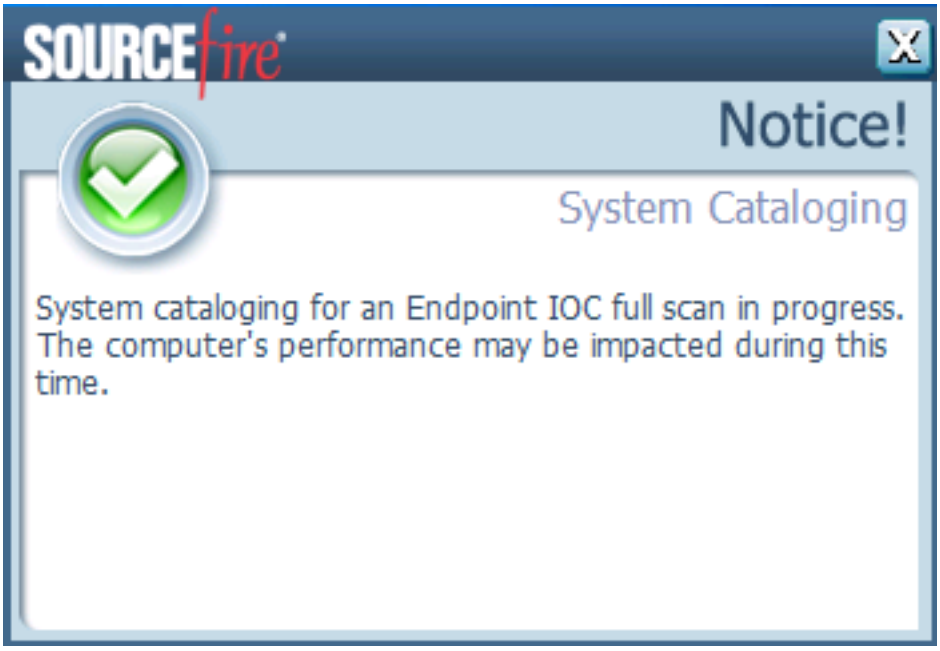


A próxima vez que esse seu PC envia uma pulsação do coração, e se suas credenciais são válidas, você deve ver um trabalho similar a este no task scheduler de Windows:



Quando a varredura começa, esta mensagem aparece:

> Nota: Se o GUI é configurado para ser hidden, a seguir você não vê a observação **catalogando do sistema**.



Quando a varredura está completa, você pode ver o *sumário da detecção da varredura do valor-limite IOC*. Este exemplo mostra um fósforo para o arquivo de assinatura de **test.txt** IOC: