Execute verificações de IOC de endpoint com AMP para endpoints ou FireAMP

Contents

Introduction

Este documento descreve como criar um arquivo de assinatura de indicação de comprometimento (IOC) através do editor de IOC Mandiant, como carregá-lo no painel do Cisco FireAMP e como iniciar uma verificação de IOC de endpoint.

Prerequisites

Requirements

A Cisco recomenda que você tenha pelo menos um gigabyte de espaço livre na unidade antes de tentar executar as verificações de IOC do endpoint.

Componentes Utilizados

As informações neste documento são baseadas no scanner IOC de endpoint, que está disponível no Cisco FireAMP Windows Connector versões 4.0.2 e posteriores.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

O recurso de scanner de IOC de endpoint é uma ferramenta poderosa de resposta a incidentes usada para verificar indicadores pós-comprometimento em vários computadores.

> **Note**: Embora o FireAMP ofereça suporte a IOCs com o idioma Mandiant, o próprio software Editor de IOC Mandiant não é desenvolvido ou suportado pela Cisco. O suporte da Cisco não soluciona problemas de IOCs criadas pelo usuário ou de terceiros.

Arquivos de assinatura IOC

O arquivo de assinatura do IOC é um esquema XML extensível para a descrição das características técnicas que identificam uma ameaça conhecida, uma metodologia de invasor ou outras evidências de comprometimento.

Você pode importar IOCs de ponto de extremidade por meio do console de arquivos baseados em OpenIOC gravados para disparar propriedades de arquivo, como nome, tamanho e hash, bem como outros atributos e propriedades do sistema, como informações de processo, serviços em execução e entradas do Registro do Microsoft Windows. A sintaxe do IOC pode ser usada pelos respondentes a incidentes para encontrar artefatos específicos ou para usar a lógica para criar detecções sofisticadas e correlacionadas para famílias de malware.

Executar uma verificação em um arquivo de assinatura IOC

Há três etapas que você deve concluir para executar uma verificação em um arquivo de assinatura IOC:

1. Crie um arquivo de assinatura IOC.
2. Carregue o arquivo de assinatura do IOC.
3. Iniciar uma análise.

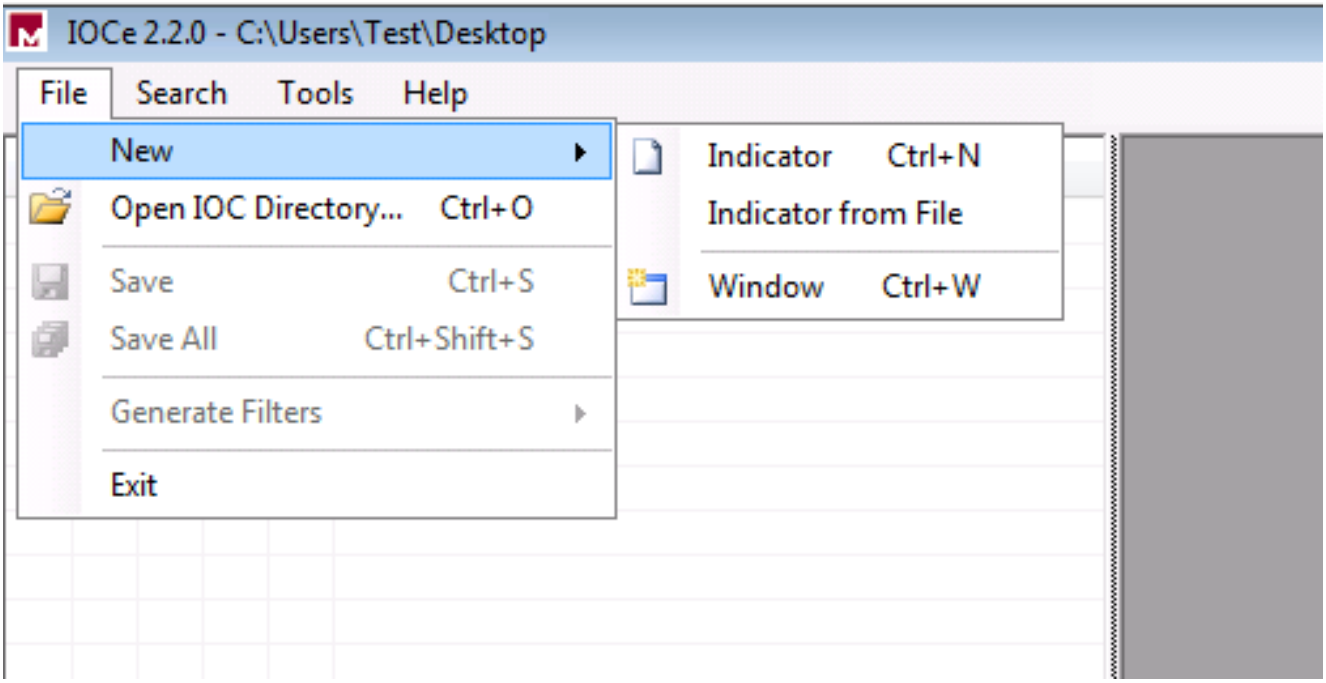
Essas etapas são expandidas nas seções a seguir.

Criar um arquivo de assinatura IOC

> **Note**: Neste exemplo, o editor de IOC Mandiant é usado para criar um arquivo de assinatura de IOC para um arquivo de texto chamado **test.txt**.

Conclua estes passos para criar um arquivo de assinatura IOC:

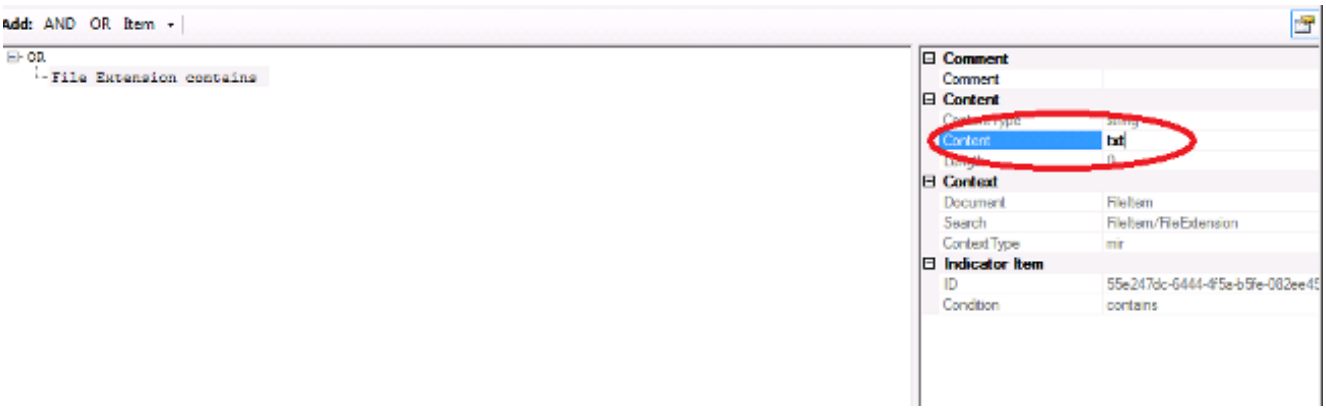
1. Abra o **IOCe** e navegue para **Arquivo > Novo > Indicador**. Isso fornece um espaço de trabalho em branco para que você possa começar a criar um IOC.



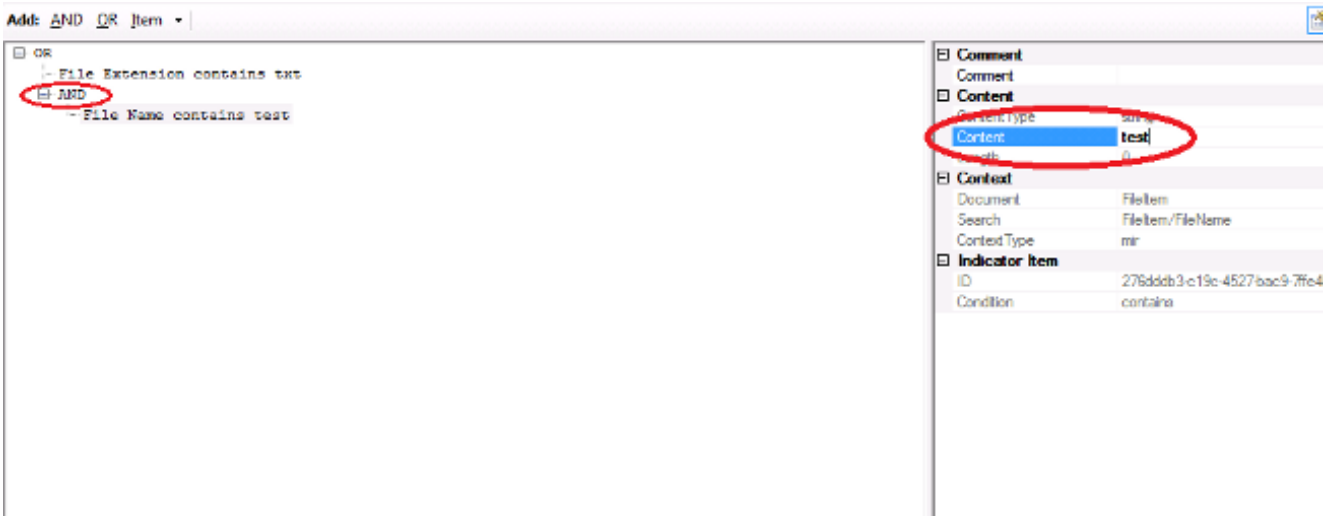
Note: Para criar um IOC para algo específico, use a lógica binária com as propriedades. O operador inicial é um OR, que é a base mais simples de se trabalhar. Isso permite que a função inicial do IOC funcione, portanto, não é necessário alterá-lo. É necessário que um arquivo de assinatura IOC tenha pelo menos duas propriedades ou condições para usá-lo com êxito em uma verificação.

2. Clique no menu suspenso **Itens** para adicionar operadores. A primeira propriedade que você deve adicionar é a **Extensão de arquivo que contém**. Localize a propriedade no menu da árvore **Itens** e clique nela.

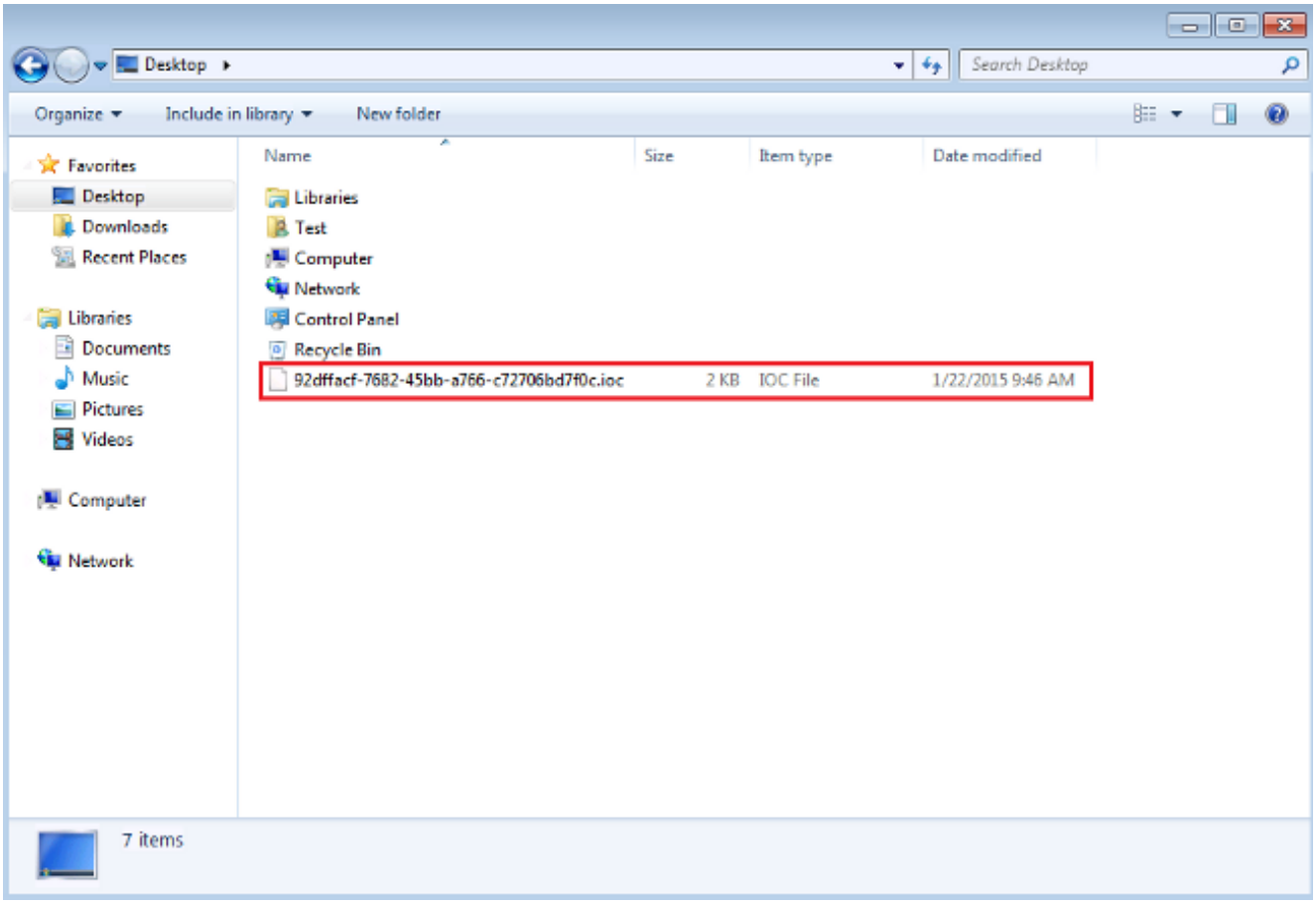
3. Depois de adicionar uma propriedade, clique no pequeno ícone no lado direito da tela para abrir o painel Configuração. Neste painel, use o campo **Conteúdo** para corresponder a uma extensão de arquivo. Por exemplo, adicione **txt** para corresponder ao arquivo de texto **test.txt**:



4. Agora você deve adicionar um operador lógico. Neste exemplo, você corresponderá ao arquivo de texto **de teste**. Para combinar isso, use um operador *AND* e adicione a próxima propriedade. Localize o nome do arquivo e selecione-o no menu da árvore **Itens**. No painel Propriedades, adicione o nome do arquivo que deseja localizar. Por exemplo, adicione o **teste** no campo Conteúdo:



5. Como não são necessárias propriedades adicionais para este IOC simples, você agora pode salvar o arquivo. Clique em **Arquivo > Salvar** e um arquivo de assinatura com uma extensão **.ioc** será salvo no sistema:



Carregar um arquivo de assinatura IOC

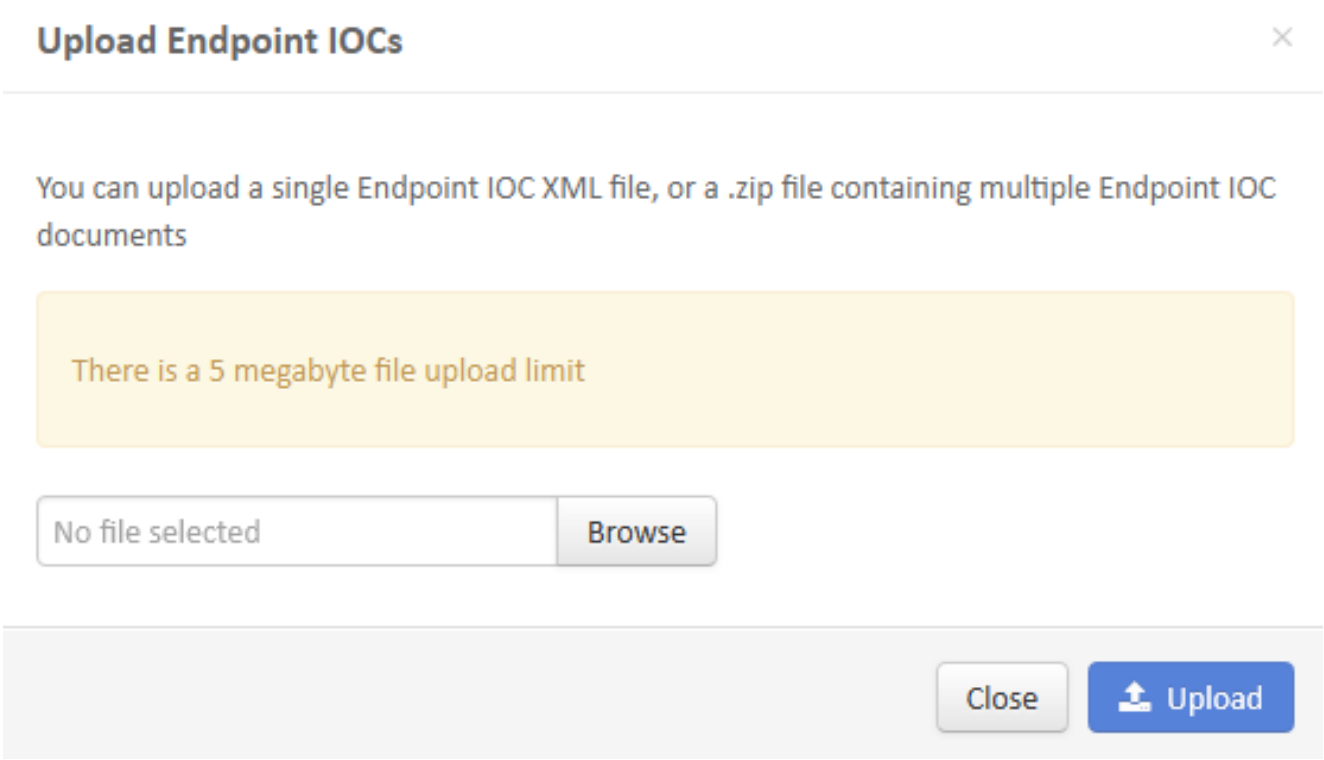
Para executar uma verificação, você deve carregar um arquivo IOC no painel do FireAMP. Você pode usar um arquivo de assinatura IOC, um arquivo XML ou um arquivo zip que contenha vários arquivos IOC. O painel descompacta e analisa o arquivo com as assinaturas do IOC. Você será notificado se uma sintaxe incorreta ou uma propriedade não suportada for usada.

Tip: Você pode carregar arquivos com até cinco megabytes de tamanho.

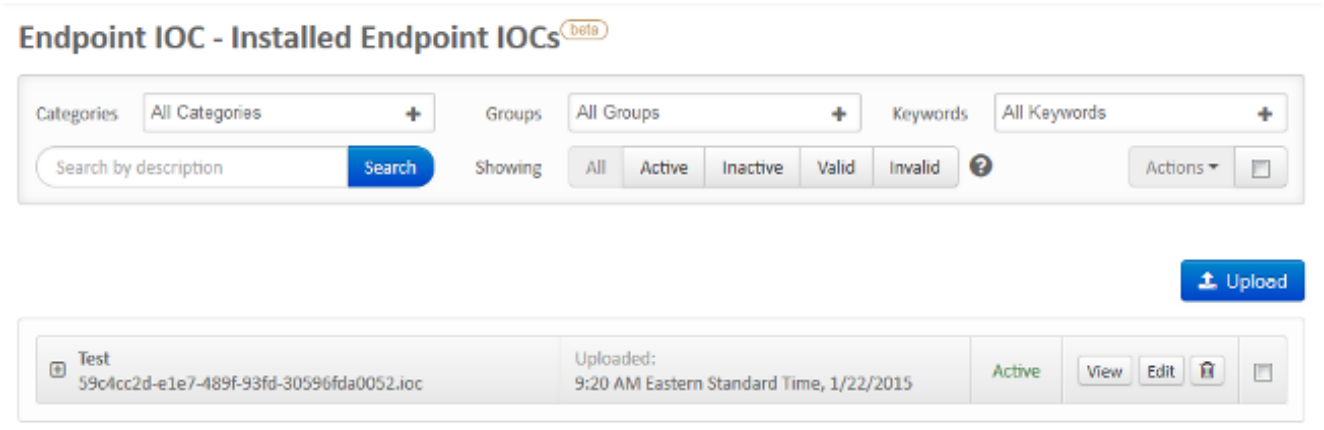
Conclua estes passos para carregar o arquivo de assinatura do IOC no painel do FireAMP:

1. Faça login no FireAMP Cloud Console e navegue até **Outbreak Control > Installed Endpoint IOC (Controle de ataques > IOC de endpoints instalados)**.

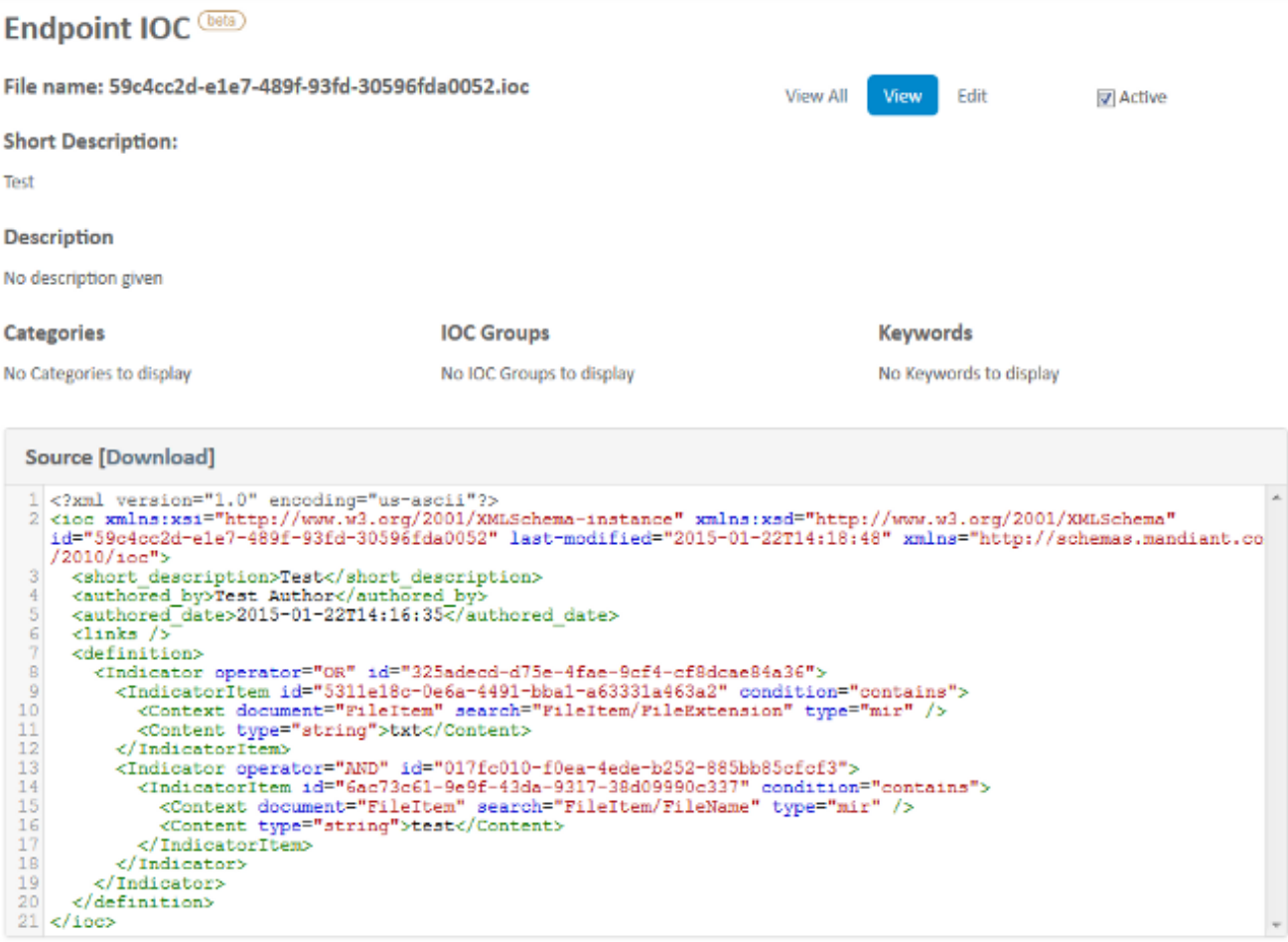
2. Clique em **Upload** e a janela **Upload Endpoint IOCs** será exibida:



Depois que um arquivo de assinatura IOC é carregado com êxito, a assinatura aparece na lista:



3. Clique em **Exibir** para exibir os dados XML reais da assinatura:



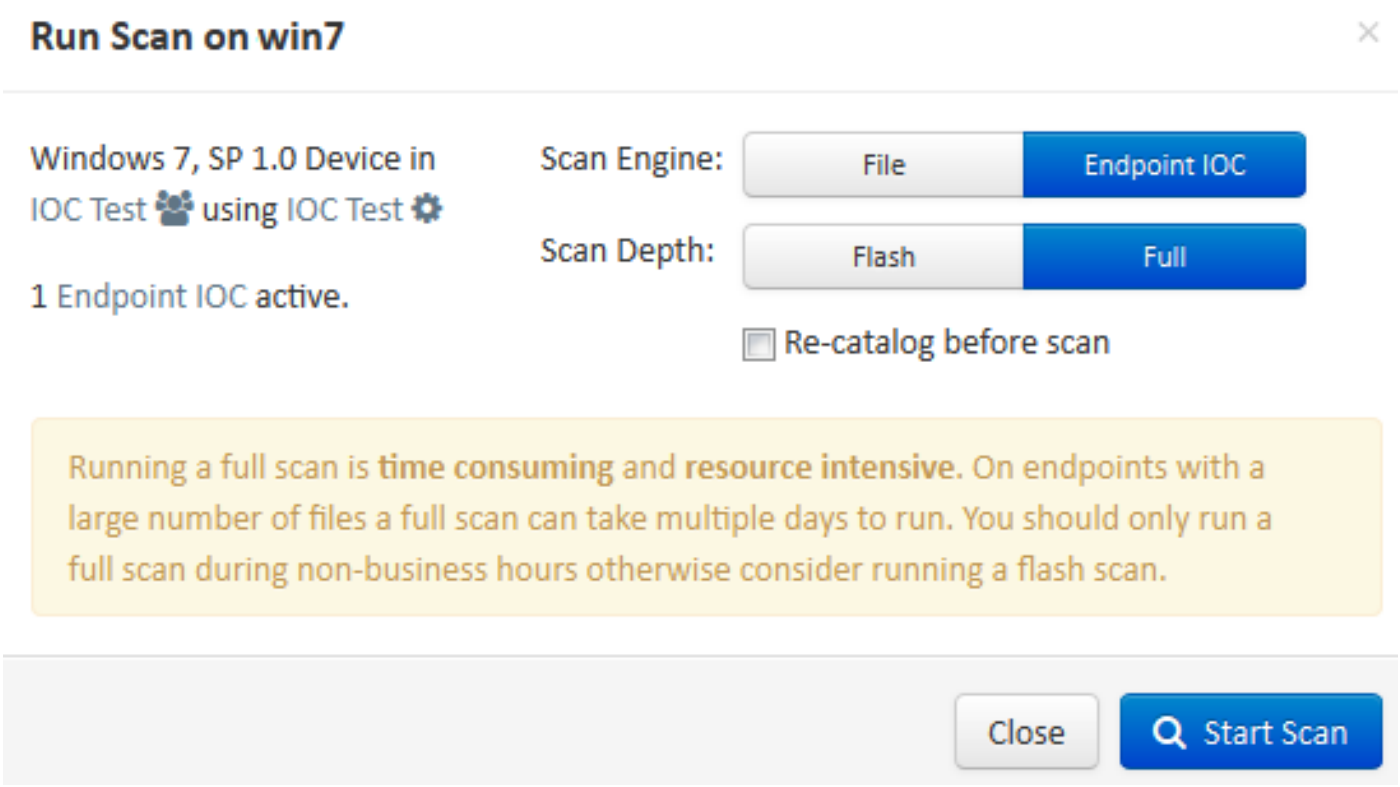
Iniciar uma digitalização

Depois de carregar um arquivo de assinatura, execute uma verificação *completa*. A primeira verificação deve ser uma verificação completa porque deve criar um catálogo de metadados para todo o computador, o que pode levar de 1 a 2 horas. Você pode executar uma verificação *flash* após o sistema ser catalogado por meio de uma verificação completa.

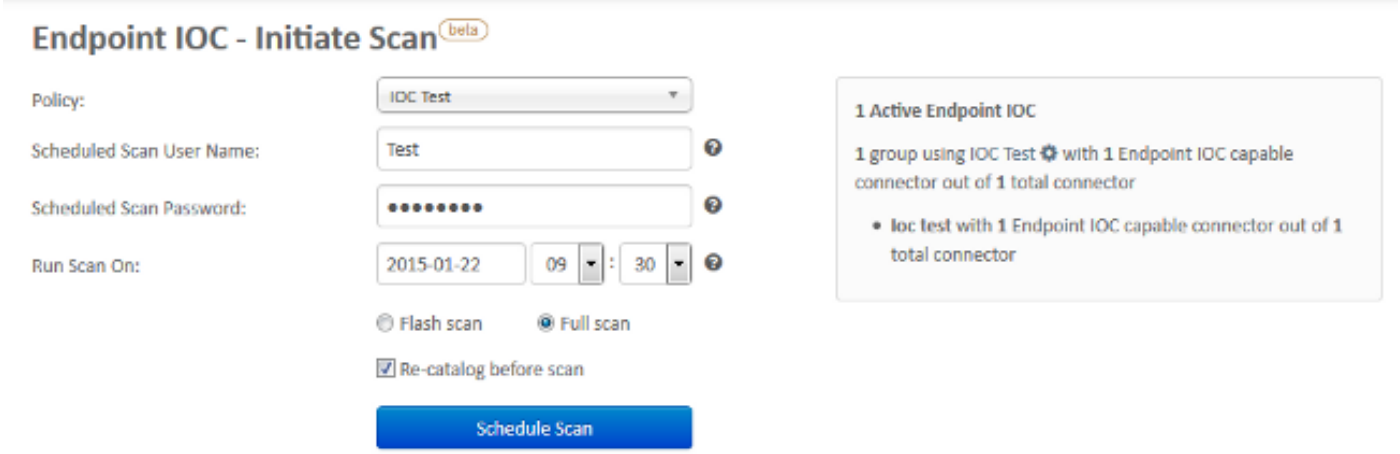
> **Note**: A verificação completa exige muito da CPU. A Cisco recomenda que você não execute uma verificação completa em um PC enquanto ele estiver em uso. Se planeja usar o recurso regularmente, você pode executar uma varredura completa uma vez por mês para reconstruir o catálogo.

Há dois métodos diferentes que você pode usar para executar uma verificação de IOC. O primeiro método é executar uma verificação imediata a partir de um evento ou do painel. Isso é acionado na próxima vez que um PC enviar um pulsar para a nuvem.

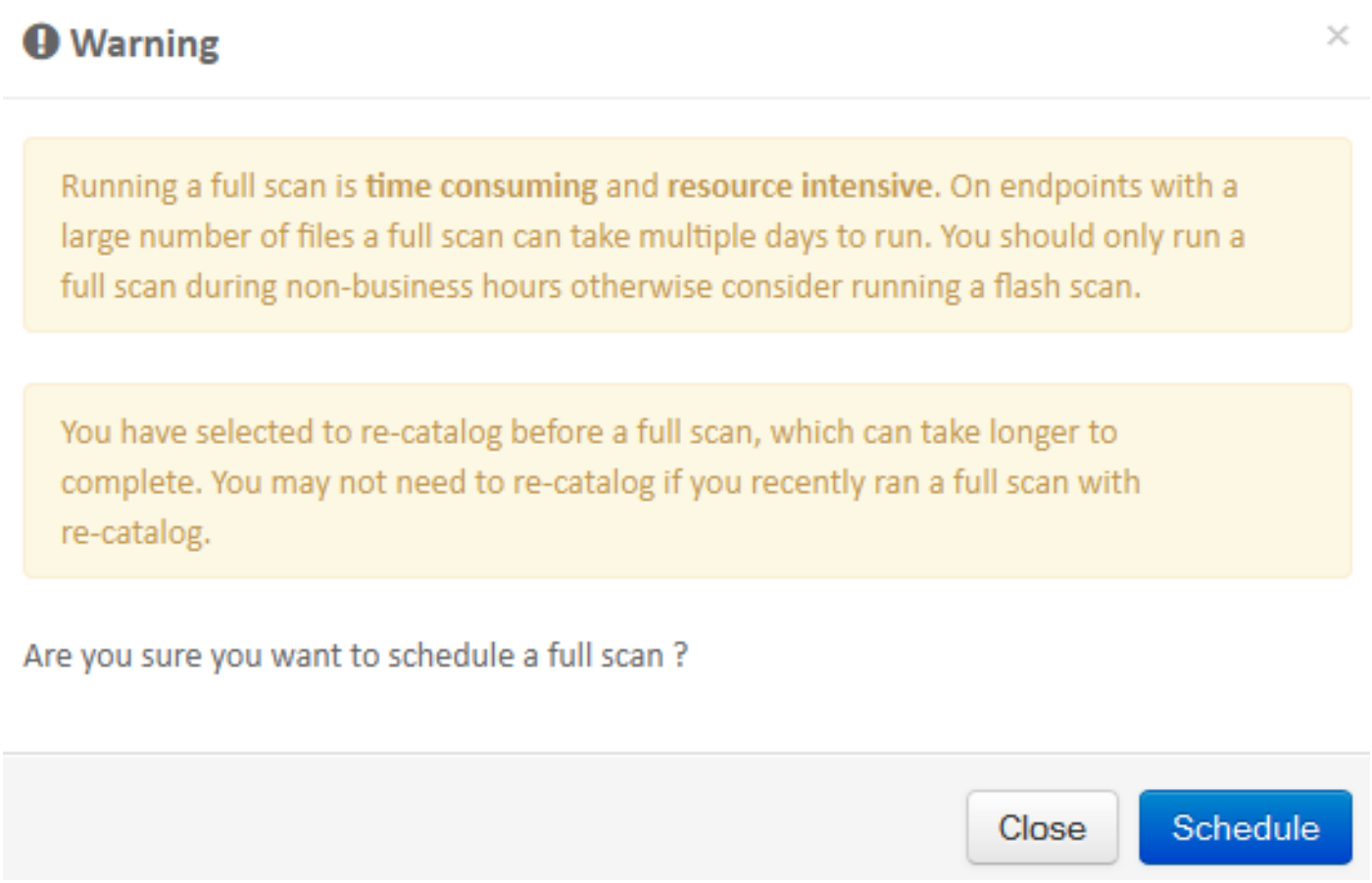
> **Note**: Se esta for a primeira vez que você executa a verificação completa, não será necessário verificar a opção **Recatalogar antes de digitalizar**.



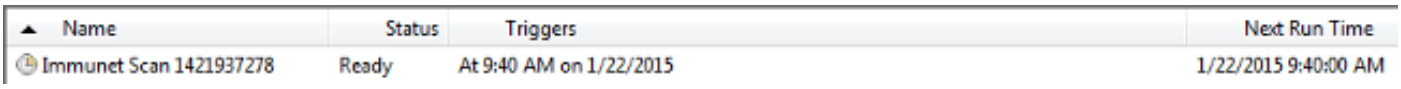
O segundo método é criar uma verificação de IOC de endpoint agendada no menu **Controle de epidemia** do painel. Essa opção pode ser ideal quando você deseja executar verificações fora do horário de pico. Tem de fornecer as credenciais de uma conta com permissão no computador especificado para criar tarefas agendadas e permitir a permissão de política de **início de sessão como** grupo de **lotes**.



Quando você agenda uma verificação de IOC de ponto final, esta mensagem de aviso é exibida:

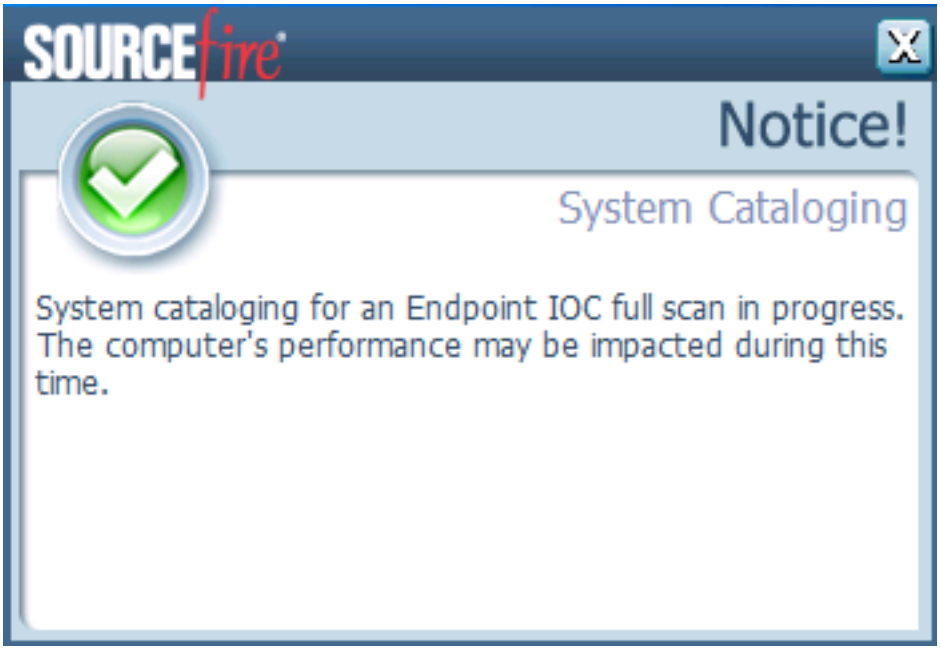


Na próxima vez em que o PC enviar um heartbeat e se suas credenciais forem válidas, você deverá ver um trabalho semelhante a este no Agendador de Tarefas do Windows:



Quando a verificação é iniciada, esta mensagem é exibida:

> **Note**: Se a GUI estiver configurada para ser oculta, você não verá o aviso **de catálogo do sistema**.



Quando a verificação estiver concluída, poderá ver o *Resumo da detecção de detecção de detecção de IOC de endpoint*. Este exemplo mostra uma correspondência para o arquivo de assinatura IOC **test.txt**: