Realice la indicación del punto final de las exploraciones del compromiso (IOC) con el AMP para los puntos finales o FireAMP

Contenido

Introducción

Este documento describe cómo crear una indicación del archivo de firma del compromiso (IOC) vía el editor de Mandiant IOC, cómo cargarlo al panel de Cisco FireAMP, y cómo iniciar una exploración del punto final IOC.

Prerequisites

Requisitos

Cisco recomienda que usted tiene por lo menos un gigabyte de espacio libre de la unidad antes de que usted intente funcionar con las exploraciones del punto final IOC.

Componentes Utilizados

La información en este documento se basa en el escáner del punto final IOC, que está disponible en las versiones 4.0.2 del conector de Cisco FireAMP Windows y posterior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando,

asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

La característica del escáner del punto final IOC es una herramienta potente de la respuesta del incidente que se utiliza para analizar los indicadores del poste-compromiso a través de las varias computadoras.

> **Note**: Aunque FireAMP soporte los IOC con el lenguaje de Mandiant, el software sí mismo del editor de Mandiant IOC no es desarrollado ni es soportado por Cisco. El soporte de Cisco no resuelve problemas los IOC creados por el usuario o de tercera persona.

Archivos de firma IOC

El archivo de firma IOC es un esquema XML extensible para la descripción de las características técnicas que identifican una amenaza sabida, una metodología del atacante, u otras pruebas del compromiso.

Usted puede importar el punto final IOC a través de la consola de los archivos OpenIOC-basados que se escriben para accionar en las propiedades del archivo tales como nombre, tamaño, y hash, así como otros atributos y propiedades Propiedad del sistema tales como información de proceso, servicios corrientes, y entradas de registro de Microsoft Windows. El sintaxis IOC se puede utilizar por los respondedores del incidente para encontrar los artefactos específicos o para utilizar la lógica para crear las detecciones sofisticadas, correlacionadas para las familias de malware.

Funcione con una exploración en un archivo de firma IOC

Hay tres pasos que usted debe completar para funcionar con una exploración en un archivo de firma IOC:

1. Cree un archivo de firma IOC.
2. Cargue el archivo de firma IOC.
3. Inicie una exploración.

Estos pasos se amplían sobre en las secciones que siguen.

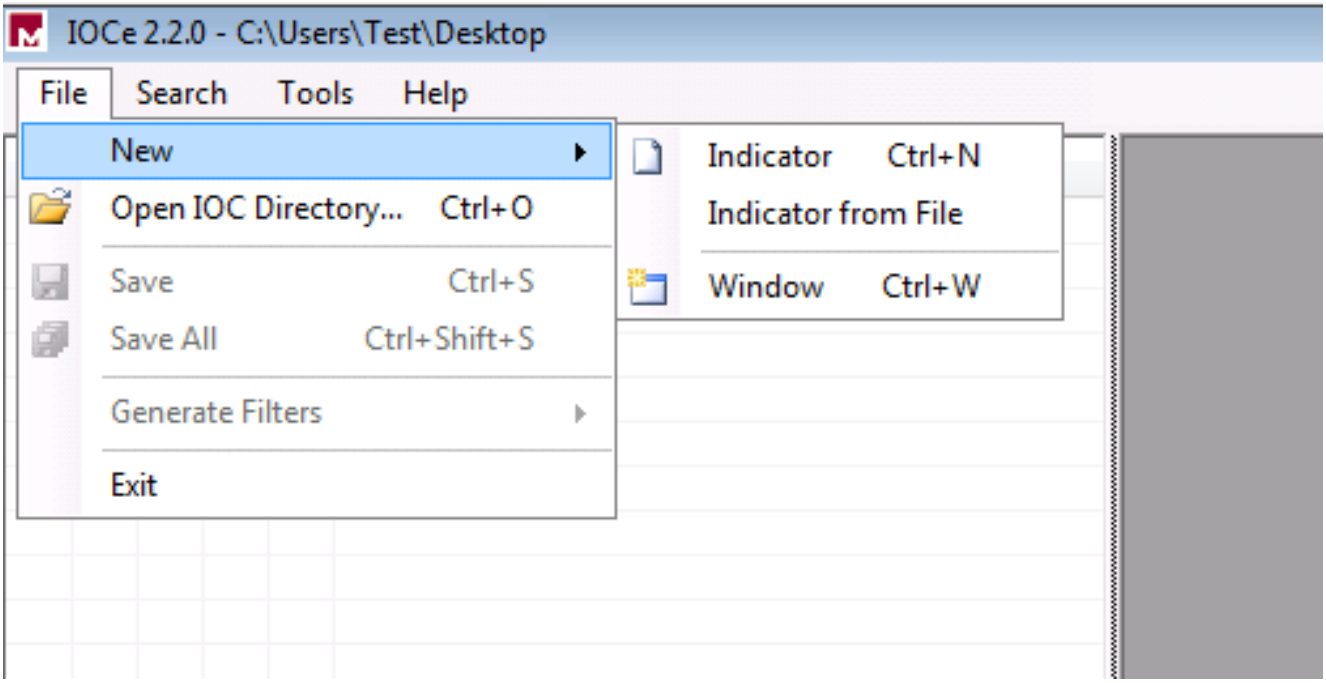
Cree un archivo de firma IOC

> **Note**: En este ejemplo, el editor de Mandiant IOC se utiliza para construir un archivo de firma IOC para un archivo de texto nombrado **test.txt**.

Complete estos pasos para crear un archivo de firma IOC:

1. Abra el **IOCe** y navegue al **indicador del File (Archivo) > New (Nuevo)**. Esto proporciona un

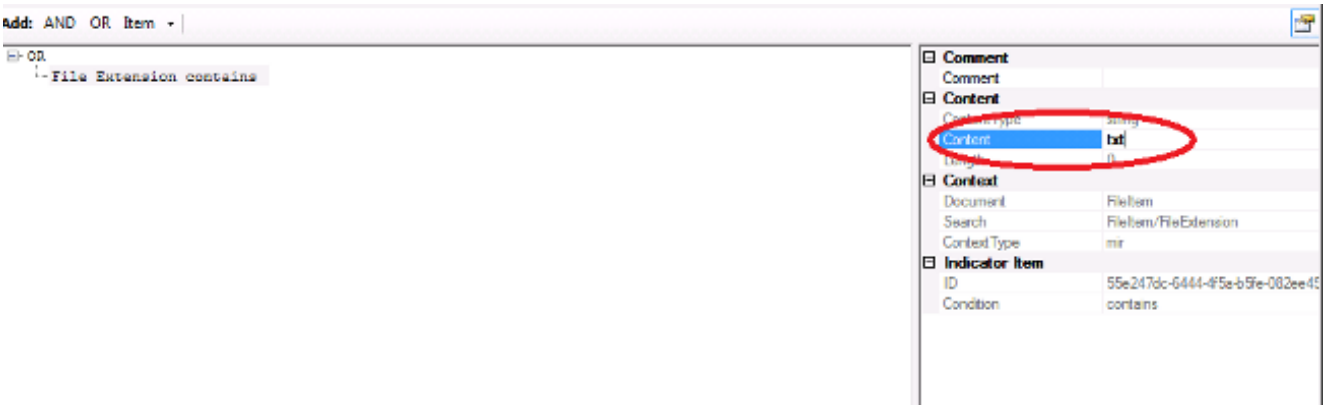
espacio de trabajo en blanco de modo que usted pueda comenzar a construir un IOC.



Note: Para crear un IOC para algo específico, utilice la lógica binaria con las propiedades. El operador inicial es O, de quien es la base más simple a trabajar. Esto permite que la función inicial del IOC trabaje, así que le no requieren cambiarlo. Se requiere que un archivo de firma IOC tiene por lo menos dos propiedades o condiciones para utilizarlo con éxito en una exploración.

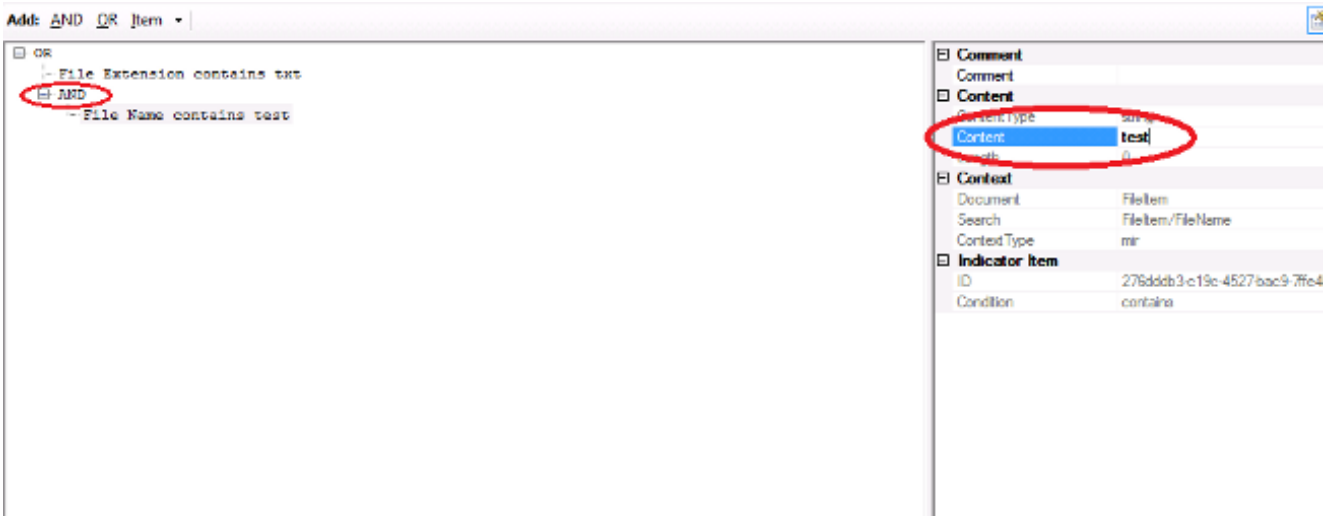
2. Haga clic el menú desplegable de los **elementos** para agregar a los operadores. La primera propiedad que usted debe agregar es **extensión de archivo contiene**. Encuentre la propiedad en el menú del árbol de los **elementos** y hágala clic.

3. Después de que usted agregue una propiedad, haga clic el pequeño icono en el lado derecho lejano de la pantalla para abrir el cristal de la configuración. Dentro de este cristal, utilice el campo **contento** para hacer juego una extensión de archivo. Por ejemplo, agregue el **txt** para hacer juego el archivo de texto de **test.txt**:

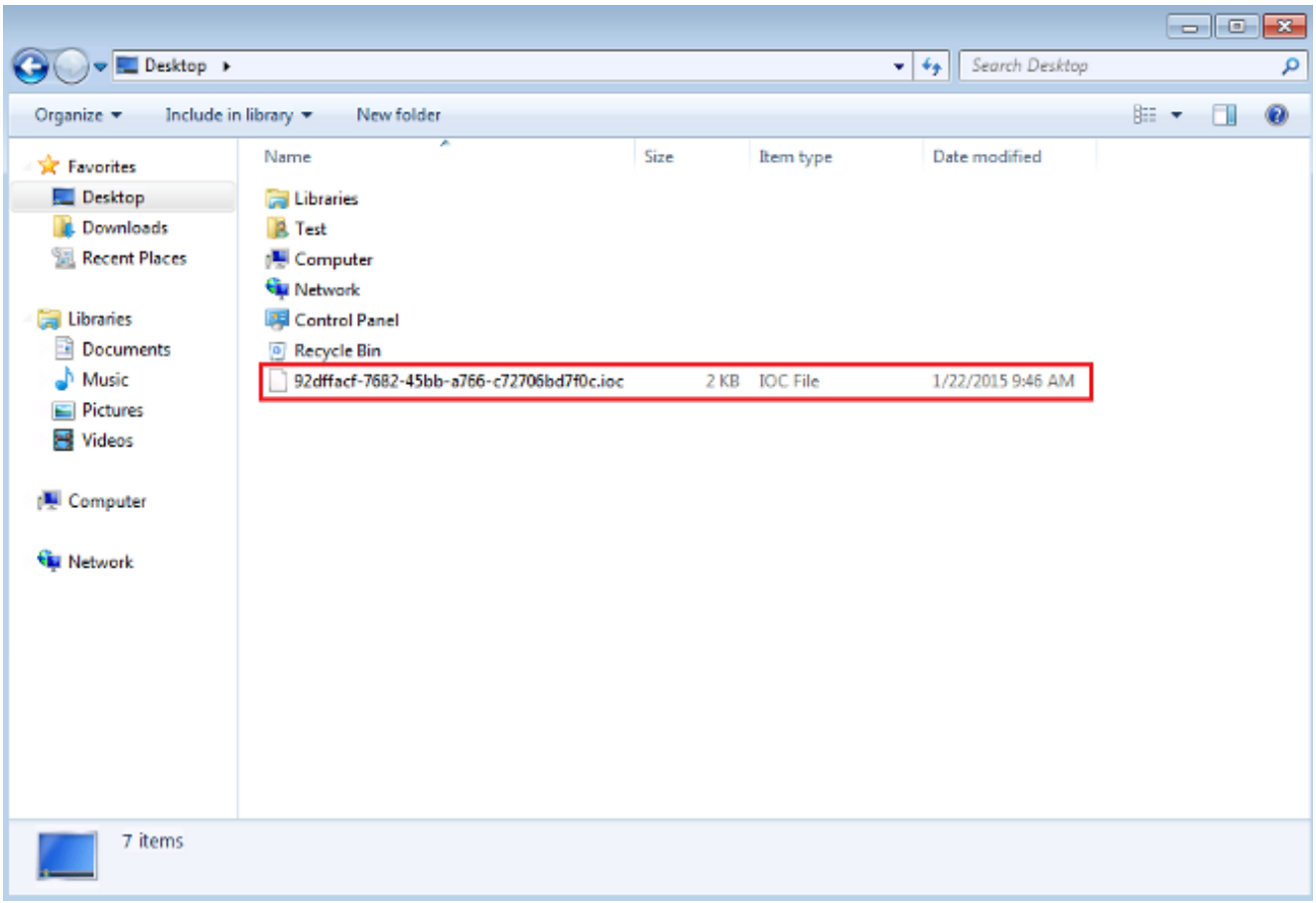


4. Usted debe ahora agregar a un operador de la lógica. En este ejemplo, usted hará juego el archivo del **texto de prueba**. Para hacer juego esto, utilice *Y al* operador y agregue la propiedad siguiente. Localice el nombre del archivo y selecciónelo del menú del árbol de los **elementos**. En el panel de propiedades, agregue el nombre del archivo que usted quiere

encontrar. Por ejemplo, agregue la **prueba** en el campo contento:



5. Puesto que no hay propiedades adicionales necesarias para este IOC simple, usted puede ahora salvar el archivo. El clic en Archivo **> la salvaguardia**, y un archivo de firma con una extensión **.ioc** se guarda en el sistema:



Cargue un archivo de firma IOC

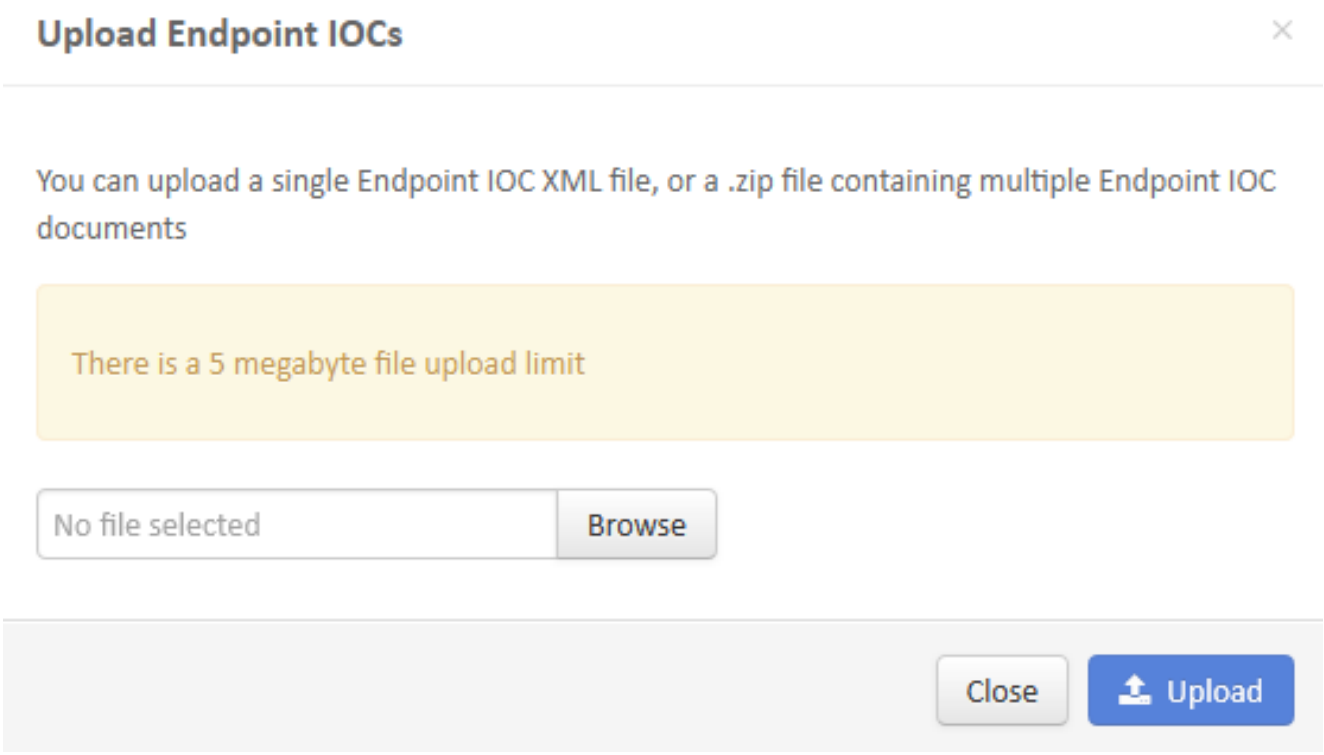
Para realizar una exploración, usted debe cargar un archivo IOC al panel de FireAMP. Usted puede utilizar un archivo de firma IOC, un archivo XML, o un archivo de la cremallera que contenga los archivos múltiples IOC. El panel descomprime y analiza el archivo con las firmas IOC. Le notifican si se utiliza una sintaxis incorrecta o una propiedad sin apoyo.

Tip: Usted puede cargar los archivos que son hasta cinco megabytes de tamaño.

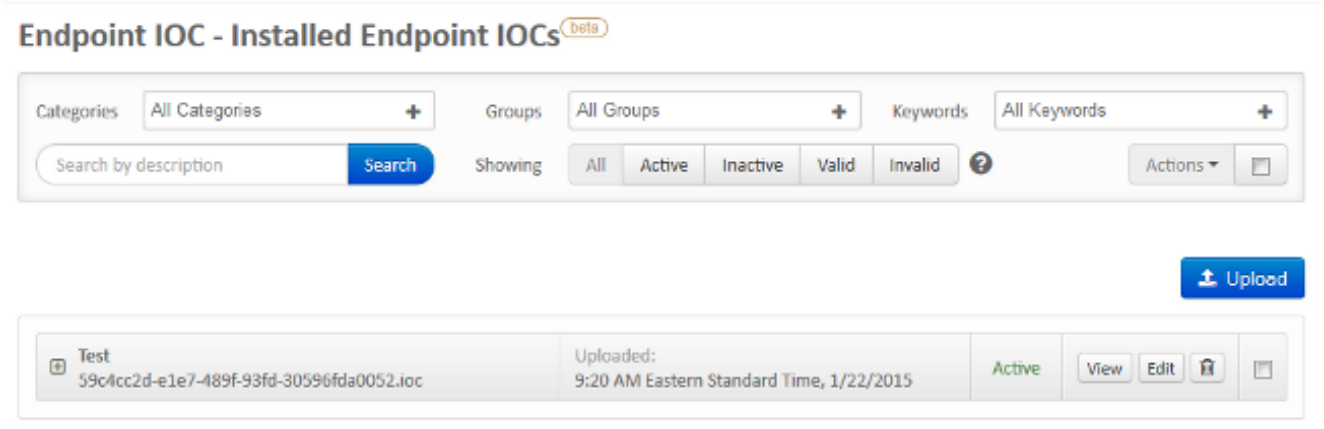
Complete estos pasos para cargar el archivo de firma IOC al panel de FireAMP:

1. El registro en la consola de la nube de FireAMP y navega al **control del brote > el punto final instalado IOC**.

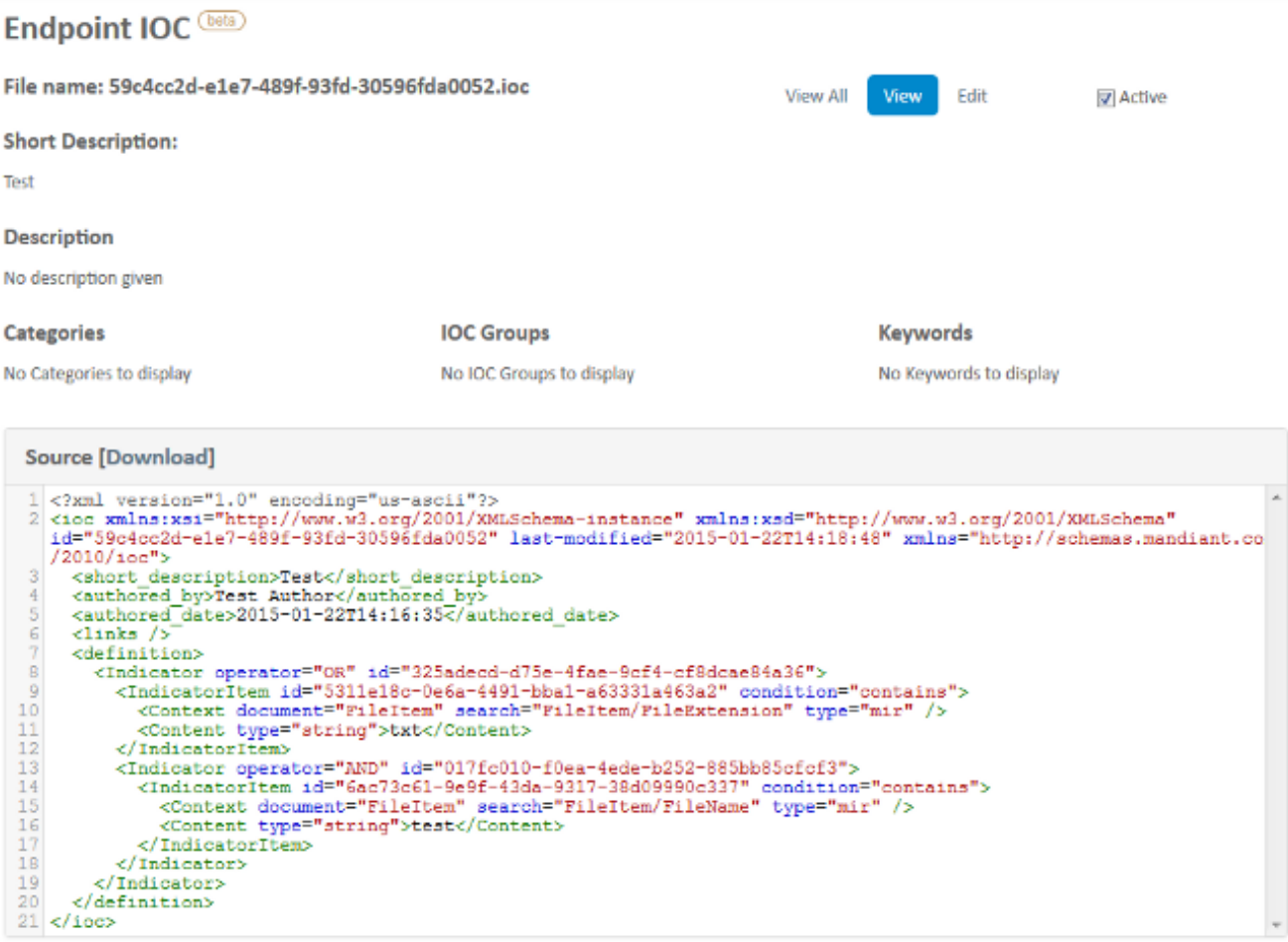
2. Haga clic la **carga**, y la ventana del **punto final IOC de la carga** aparece:



Después de que un archivo de firma IOC esté cargado con éxito, la firma aparece en la lista:



3. Haga clic la **visión** para ver los datos XML reales de la firma:



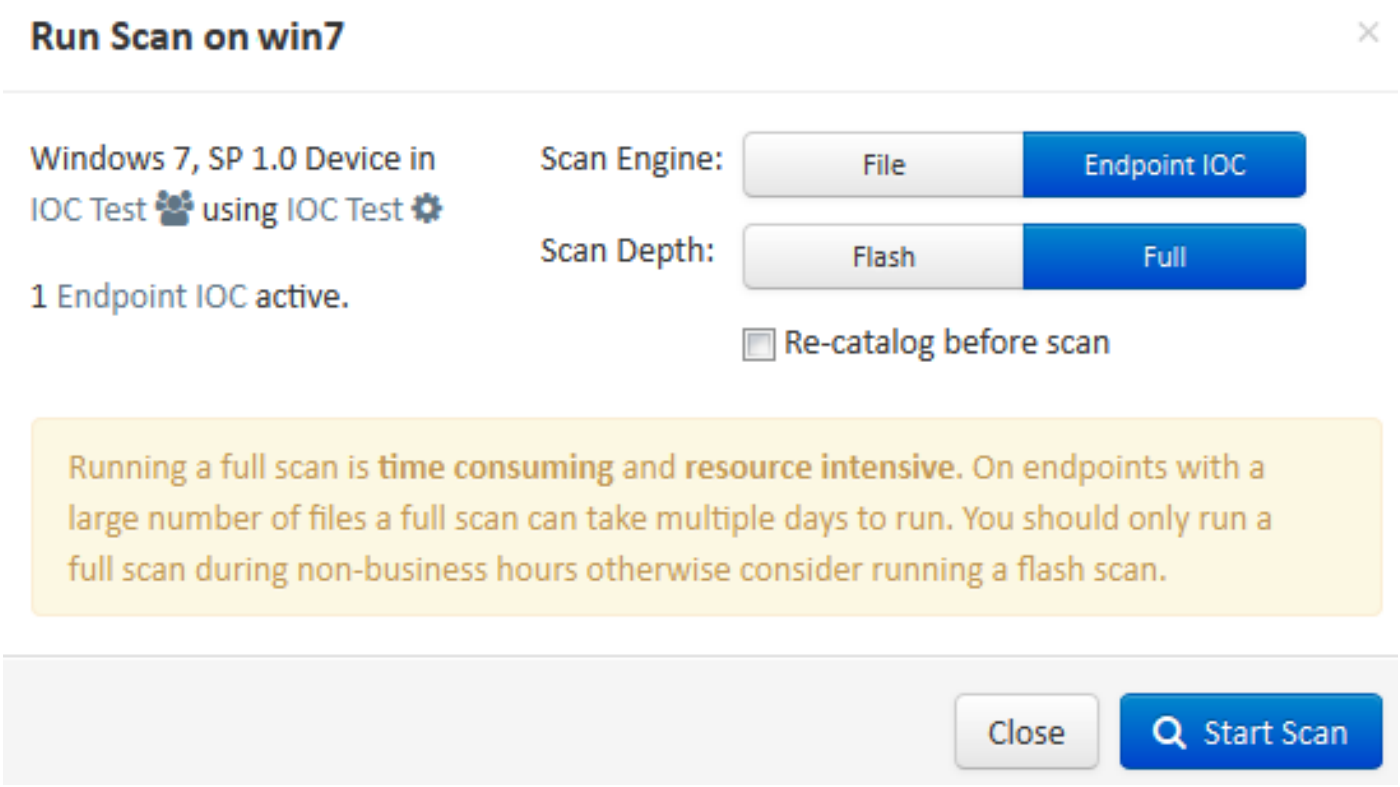
Inicie una exploración

Después de que usted cargue un archivo de firma, realice una exploración *completa*. La primera exploración debe ser una exploración completa porque debe construir un catálogo de los meta datos para el ordenador entero, que puede tardar 1 – 2 horas. Usted puede realizar una exploración *de destello* después de que el sistema se catalogue con una exploración completa.

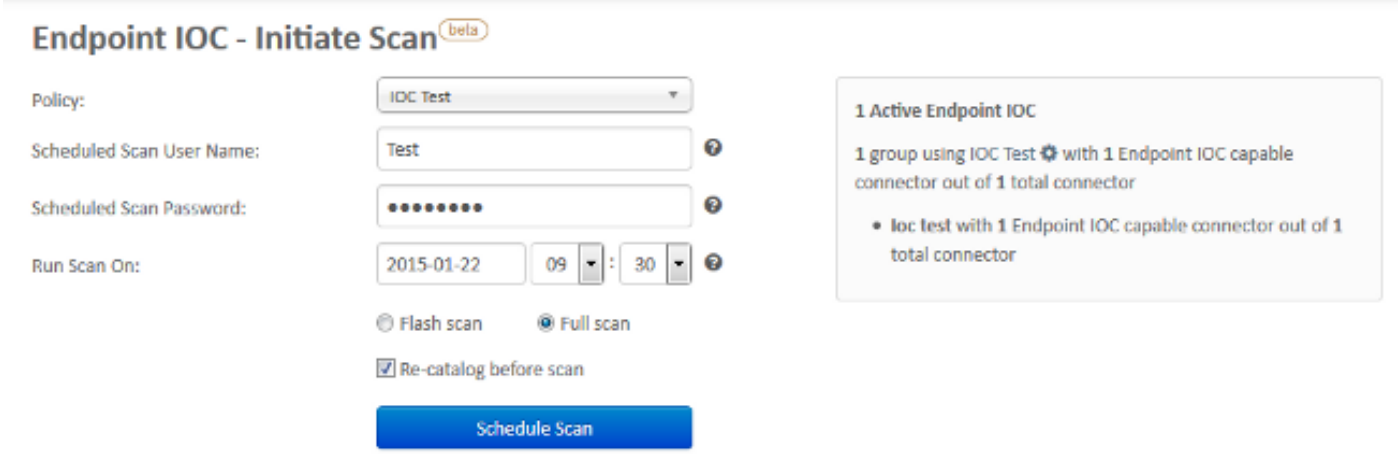
> **Note**: La exploración completa es mismo uso intensivo de la CPU. Cisco recomienda que usted no funciona con una exploración completa en un PC mientras que es funcionando. Si usted planea utilizar la característica regularmente, usted puede realizar una exploración completa una vez al mes para reconstruir el catálogo.

Hay dos métodos distintos que usted puede utilizar para funcionar con una exploración IOC. El primer método es realizar una exploración inmediata de un evento o del panel. El se acciona la próxima vez que un PC envía un latido del corazón a la nube.

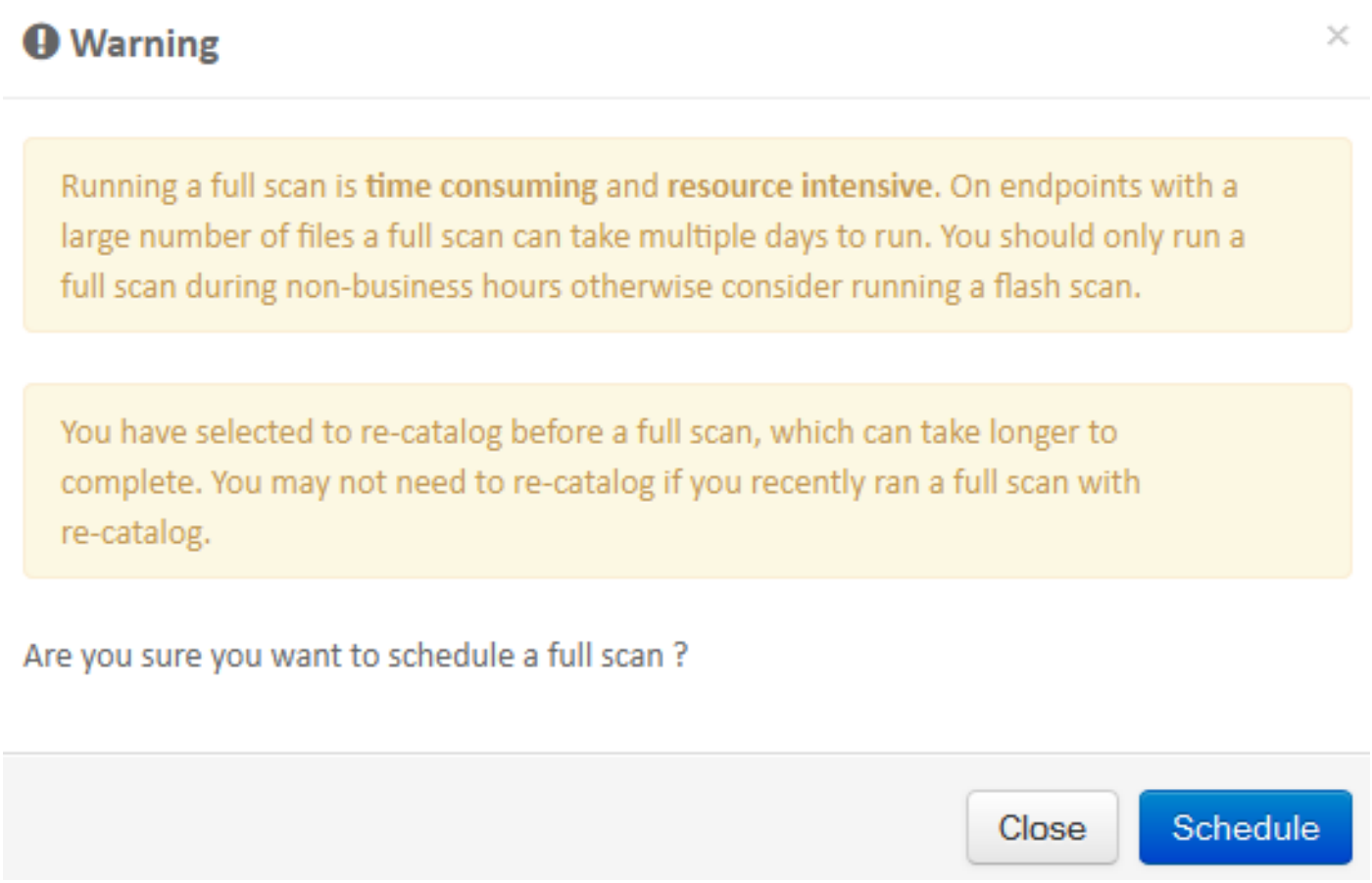
> **Note**: Si éste es la primera vez que usted funciona con la exploración completa, le no requieren marcar el **volver a catalogar antes de la** opción de la **exploración**.



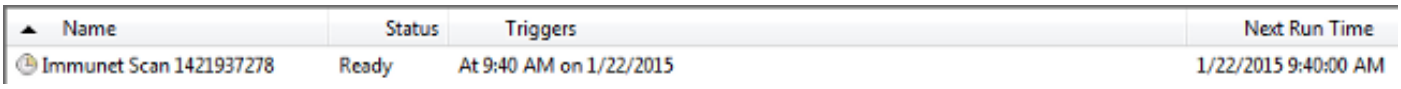
El segundo método es crear una exploración programada del punto final IOC del **menú de control del brote del** panel. Esta opción pudo ser ideal cuando usted desea de realizar las exploraciones durante las horas no pico. Usted debe proporcionar las credenciales de una cuenta que tenga permiso en el ordenador dado para crear Scheduled Tasks y permitir el **inicio pues** permiso de la directiva del grupo del **lote**.



Cuando usted programa una exploración del punto final IOC, este mensaje de advertencia aparece:

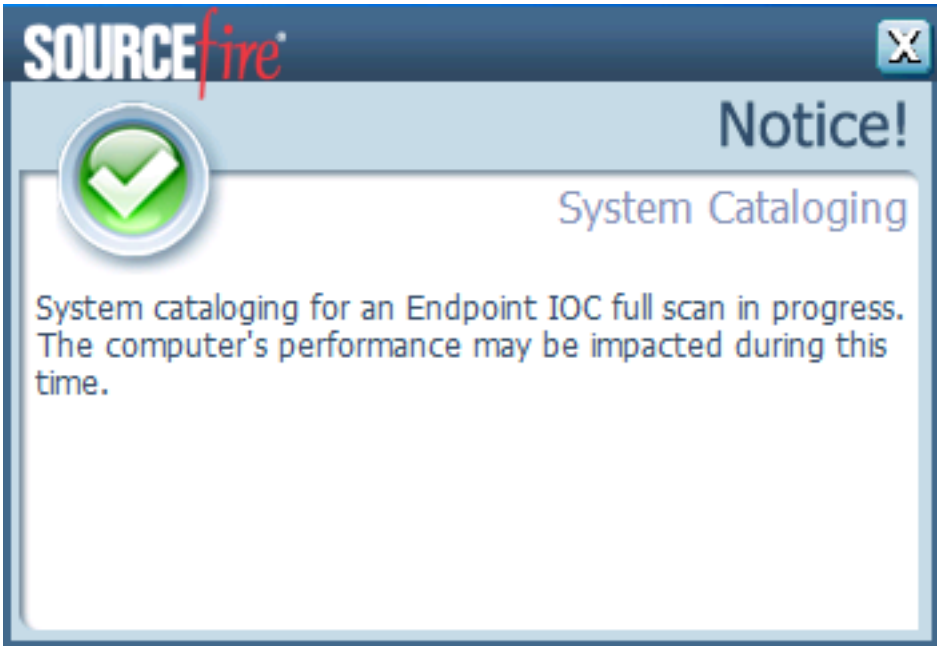


La próxima vez que ese su PC envía un latido del corazón, y si sus credenciales son válidas, usted debe ver un trabajo similar a esto en el Programador de tareas de Windows:



Cuando la exploración comienza, este mensaje aparece:

> **Note**: Si el GUI se configura para ser ocultado, después usted no ve el aviso de **catalogación del sistema**.



Cuando la exploración es completa, usted puede ver el *resumen de la detección de la exploración del punto final IOC*. Este ejemplo muestra una coincidencia para el archivo de firma de **test.txt** IOC: