Realizar análisis IOC de terminales con AMP para terminales o FireAMP

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Archivos de firma IOC](#)
[Ejecutar un análisis en un archivo de firma IOC](#)
[Crear un archivo de firma IOC](#)
[Cargar un archivo de firma IOC](#)
[Iniciar un análisis](#)

Introducción

Este documento describe cómo crear un archivo de firma de indicación de compromiso (IOC) a través del editor de IOC de Mandiant, cómo cargarlo en el panel de Cisco FireAMP y cómo iniciar un escaneo de IOC de terminal.

Prerequisites

Requirements

Cisco recomienda que tenga al menos un gigabyte de espacio libre en la unidad antes de intentar ejecutar las exploraciones IOC del terminal.

Componentes Utilizados

La información de este documento se basa en el escáner IOC del terminal, que está disponible en las versiones 4.0.2 y posteriores de Cisco FireAMP Windows Connector.

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.

Antecedentes

La función de escáner IOC del terminal es una potente herramienta de respuesta ante incidentes que se utiliza para analizar los indicadores posteriores al ataque en varios ordenadores.

> **Nota:** Aunque FireAMP admite IOC con el lenguaje Mandiant, Cisco no ha desarrollado ni admitido el software del Editor de IOC de Mandiant. El soporte de Cisco no soluciona problemas de IOC creados por el usuario o de terceros.

Archivos de firma IOC

El archivo de firma IOC es un esquema XML extensible para la descripción de características técnicas que identifican una amenaza conocida, una metodología de atacante u otra evidencia de compromiso.

Puede importar IOC de terminal a través de la consola desde los archivos basados en OpenIOC que se escriben para activar propiedades de archivo como nombre, tamaño y hash, así como otros atributos y propiedades del sistema como información de proceso, servicios en ejecución y entradas del Registro de Microsoft Windows. Los respondedores de incidentes pueden utilizar la sintaxis de IOC para encontrar artefactos específicos o para utilizar la lógica para crear detecciones sofisticadas y correlacionadas para familias de malware.

Ejecutar un análisis en un archivo de firma IOC

Hay tres pasos que debe completar para ejecutar un escaneo en un archivo de firma IOC:

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

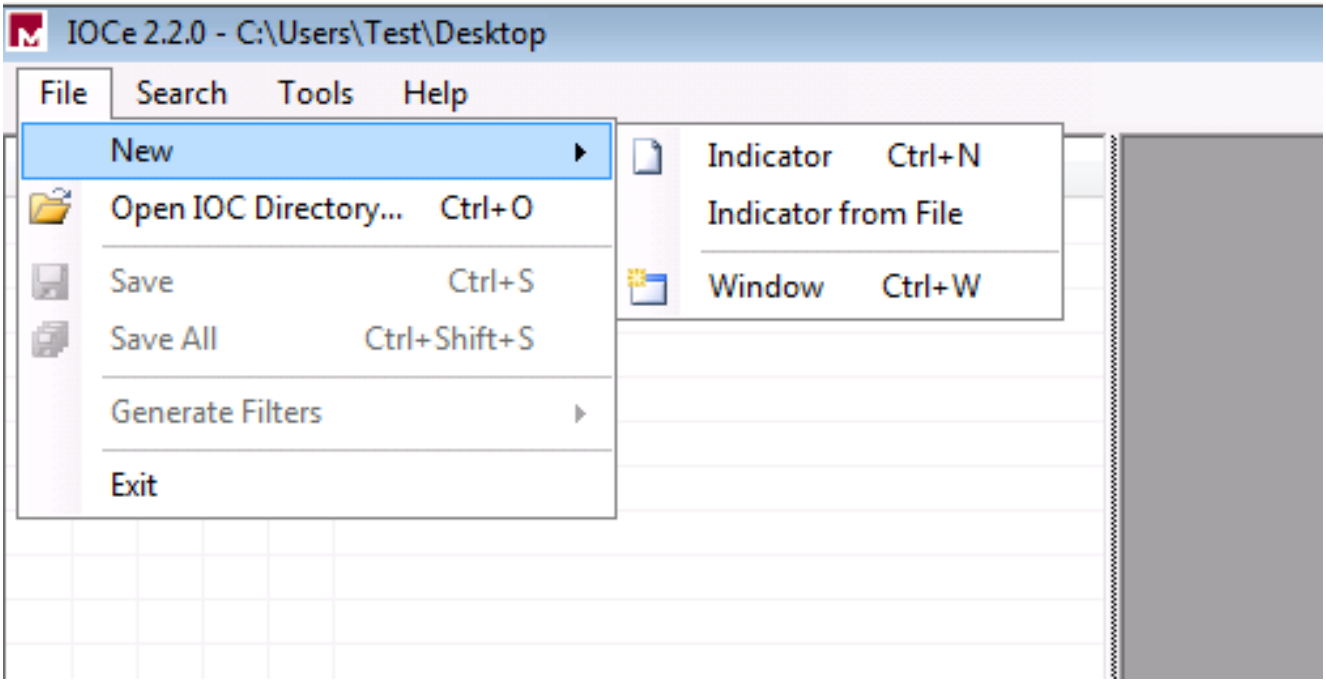
Estos pasos se amplían en las secciones siguientes.

Crear un archivo de firma IOC

> **Nota:** En este ejemplo, se utiliza el editor de IOC de Mandiant para generar un archivo de firma IOC para un archivo de texto denominado **test.txt**.

Complete estos pasos para crear un archivo de firma IOC:

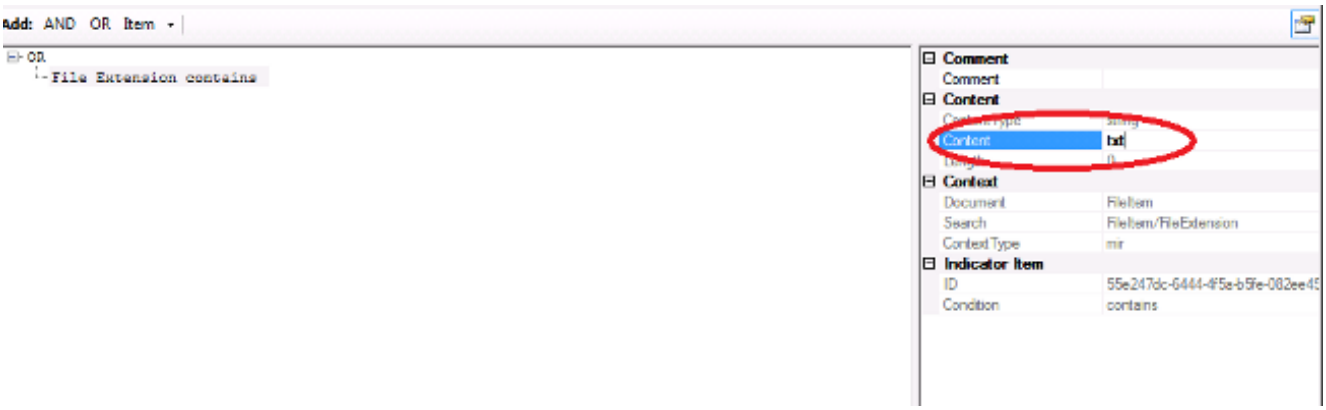
1. Abra el **IOCe** y navegue hasta **Archivo > Nuevo > Indicador**. Esto proporciona un espacio de trabajo en blanco para que pueda comenzar a generar un IOC.



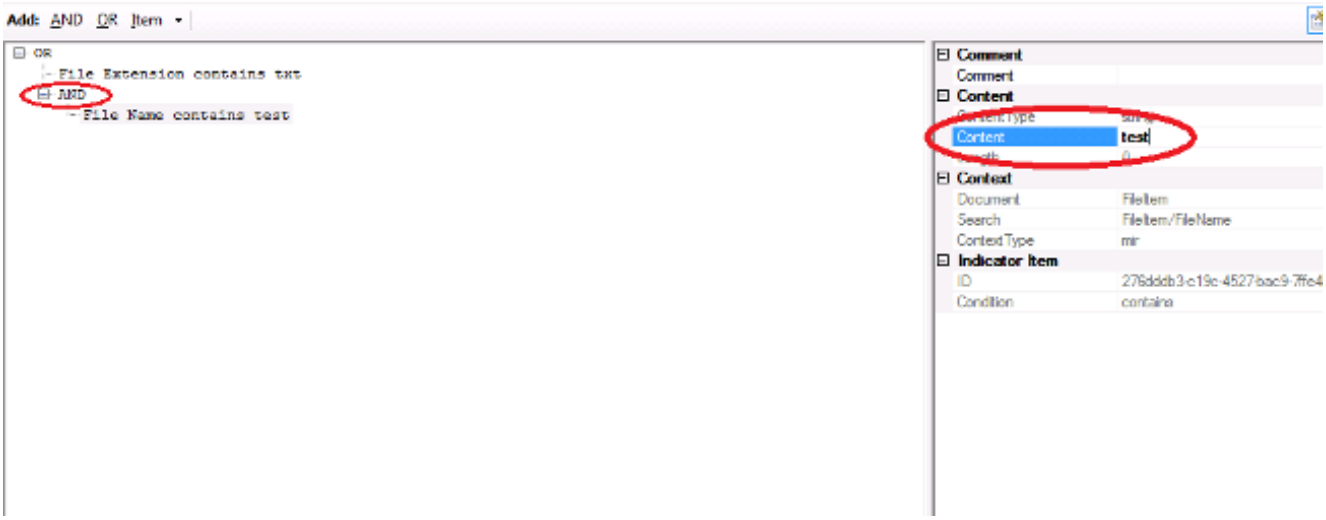
Nota: Para crear un IOC para algo específico, utilice lógica binaria con las propiedades. El operador inicial es un OR, que es la base más sencilla desde la que trabajar. Esto permite que funcione la función inicial del COI, por lo que no es necesario que la cambie. Se requiere que un archivo de firma IOC tenga al menos dos propiedades o condiciones para utilizarlo correctamente en una exploración.

2. Haga clic en el menú desplegable **Elementos** para agregar operadores. La primera propiedad que debe agregar es **File Extension**. Busque la propiedad en el menú **Elementos** y haga clic en ella.

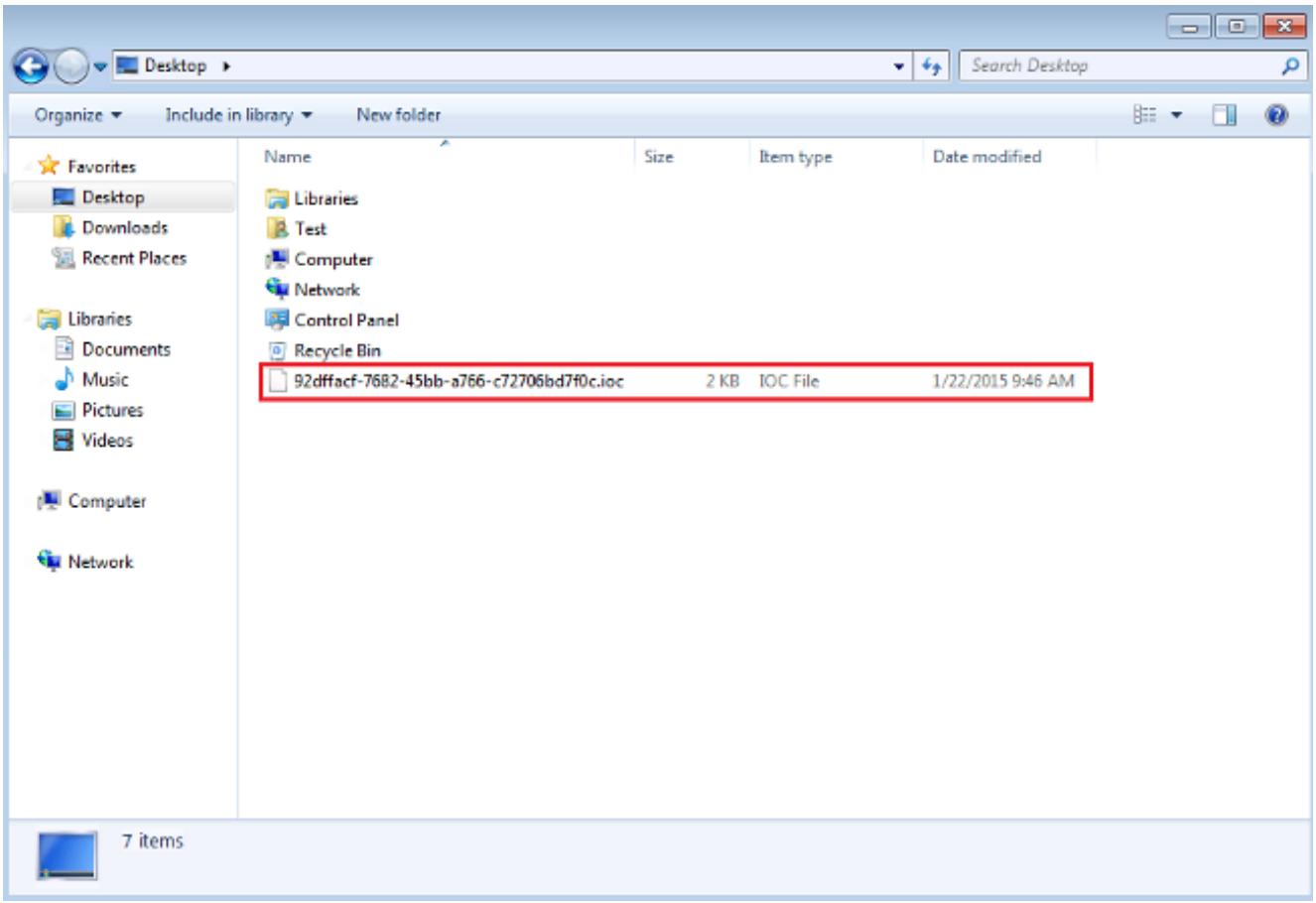
3. Después de agregar una propiedad, haga clic en el pequeño icono situado en el extremo derecho de la pantalla para abrir el panel Configuración. Dentro de este panel, utilice el campo **Content** para hacer coincidir una extensión de archivo. Por ejemplo, agregue **txt** para que coincida con el archivo de texto **test.txt**:



4. Ahora debe agregar un operador lógico. En este ejemplo, coincidirá con el archivo **de** texto **de prueba**. Para hacer coincidir esto, utilice un operador *AND* y agregue la propiedad siguiente. Localice el nombre del archivo y selecciónelo en el menú **Elementos** del árbol. En el panel Propiedades, agregue el nombre del archivo que desea buscar. Por ejemplo, agregue la **prueba** en el campo Contenido:



5. Dado que no se necesitan propiedades adicionales para este IOC simple, ahora puede guardar el archivo. Haga clic en **Archivo > Guardar** y se guardará en el sistema un archivo de firma con una extensión **.ioc**:



Cargar un archivo de firma IOC

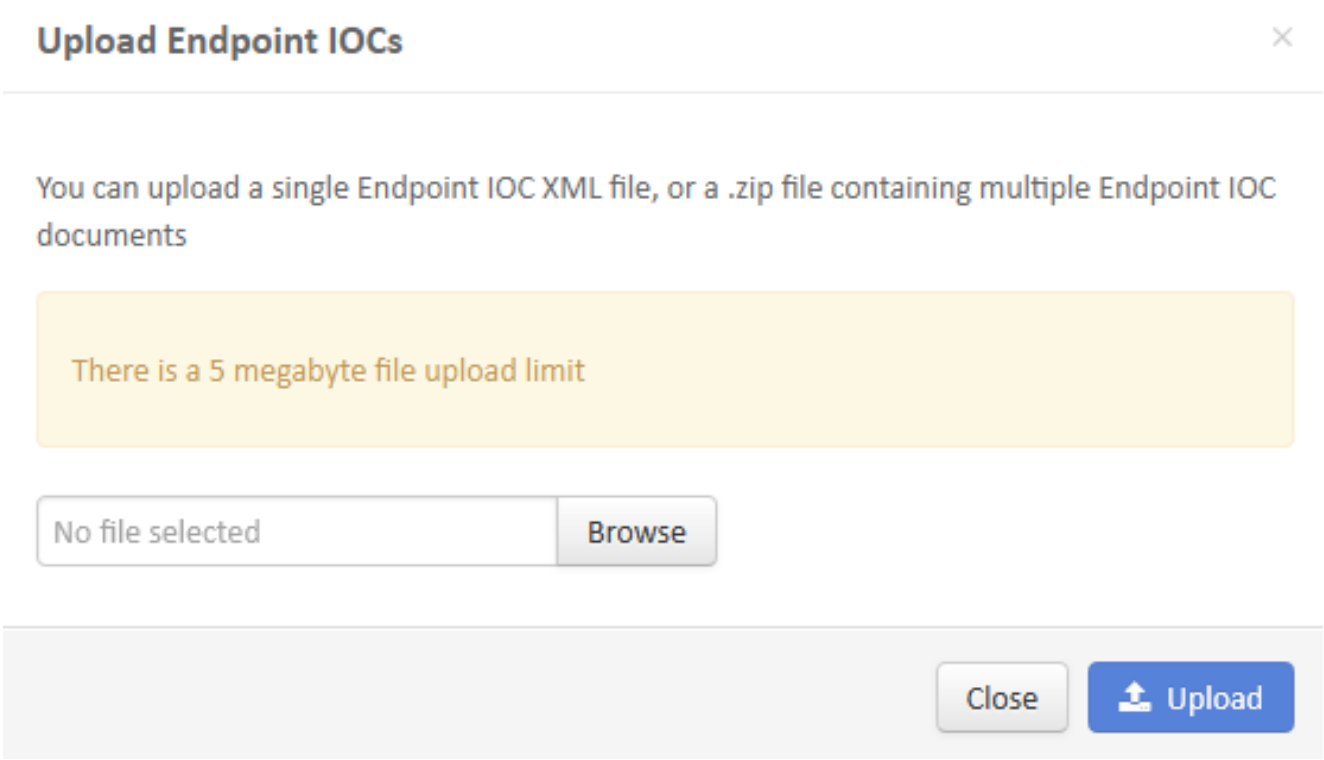
Para realizar una exploración, debe cargar un archivo IOC en el panel de FireAMP. Puede utilizar un archivo de firma IOC, un archivo XML o un archivo zip que contenga varios archivos IOC. El panel descomprime y analiza el archivo con las firmas de IOC. Se le notifica si se utiliza una sintaxis incorrecta o una propiedad no admitida.

Consejo: Puede cargar archivos de hasta cinco megabytes de tamaño.

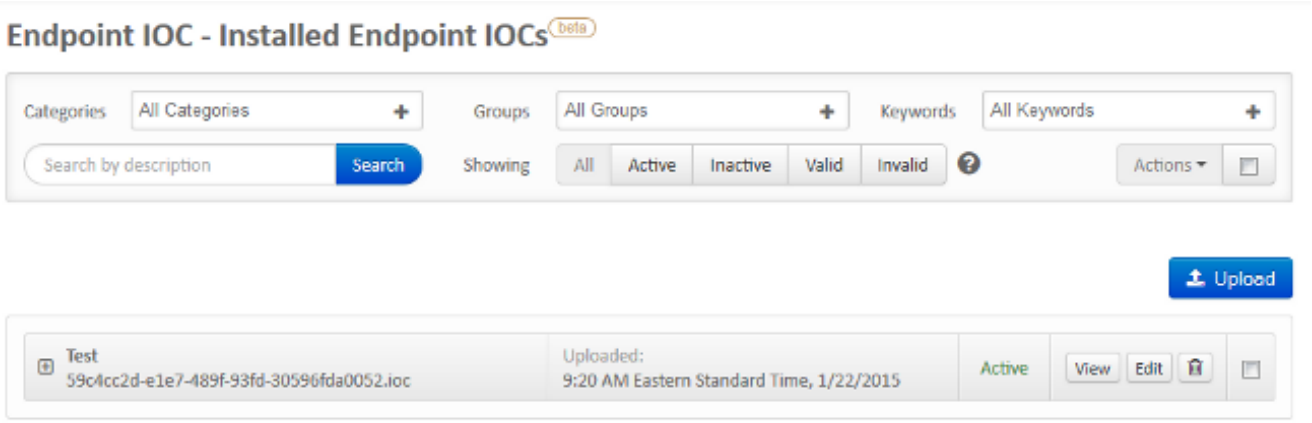
Complete estos pasos para cargar el archivo de firma IOC en el panel de FireAMP:

1. Inicie sesión en FireAMP Cloud Console y navegue hasta **Control de brotes > IOC de terminal instalado**.

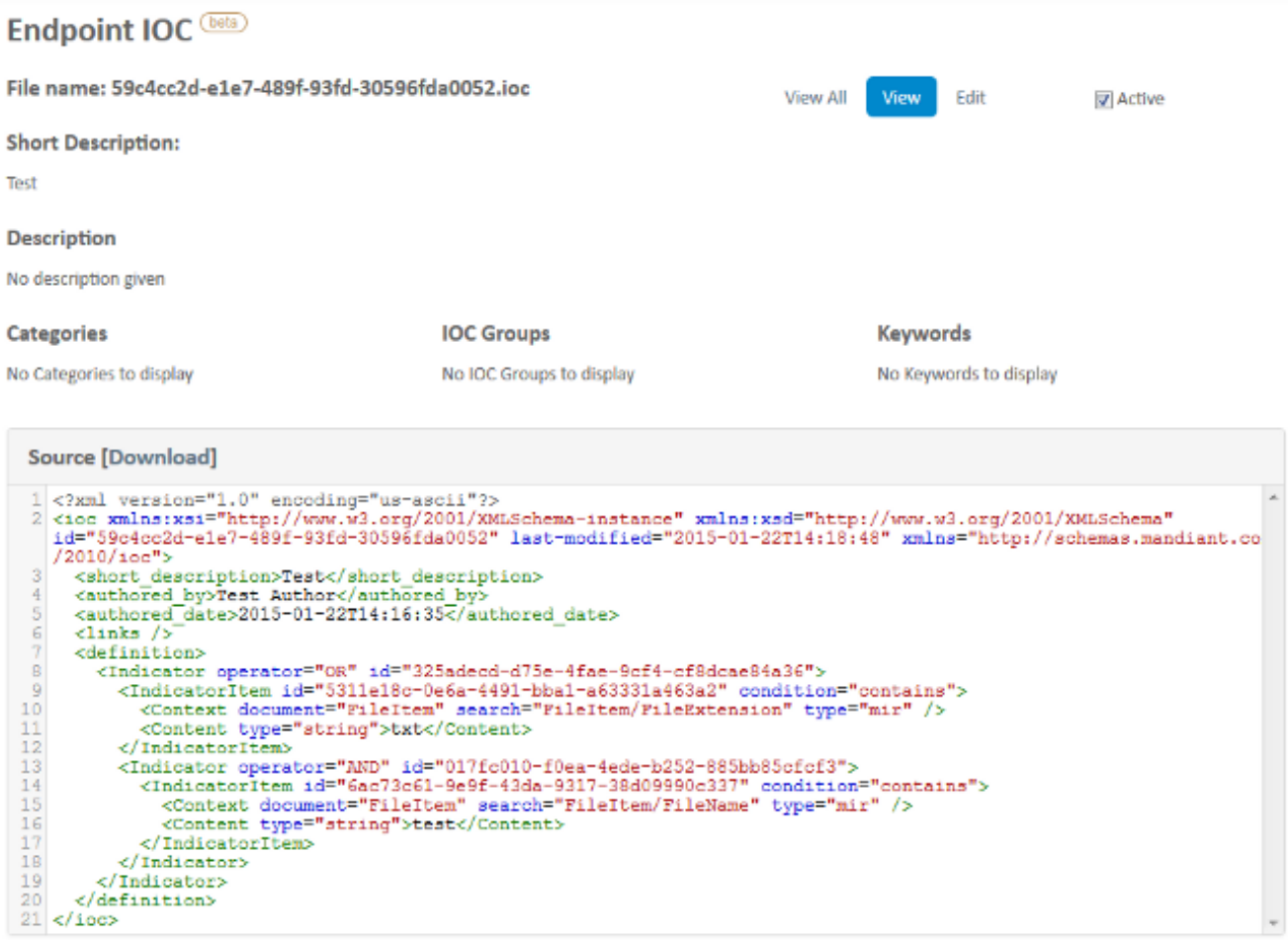
2. Haga clic en **Cargar** y aparecerá la ventana **Cargar IOC de terminal**:



Después de cargar correctamente un archivo de firma IOC, aparece la firma en la lista:



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



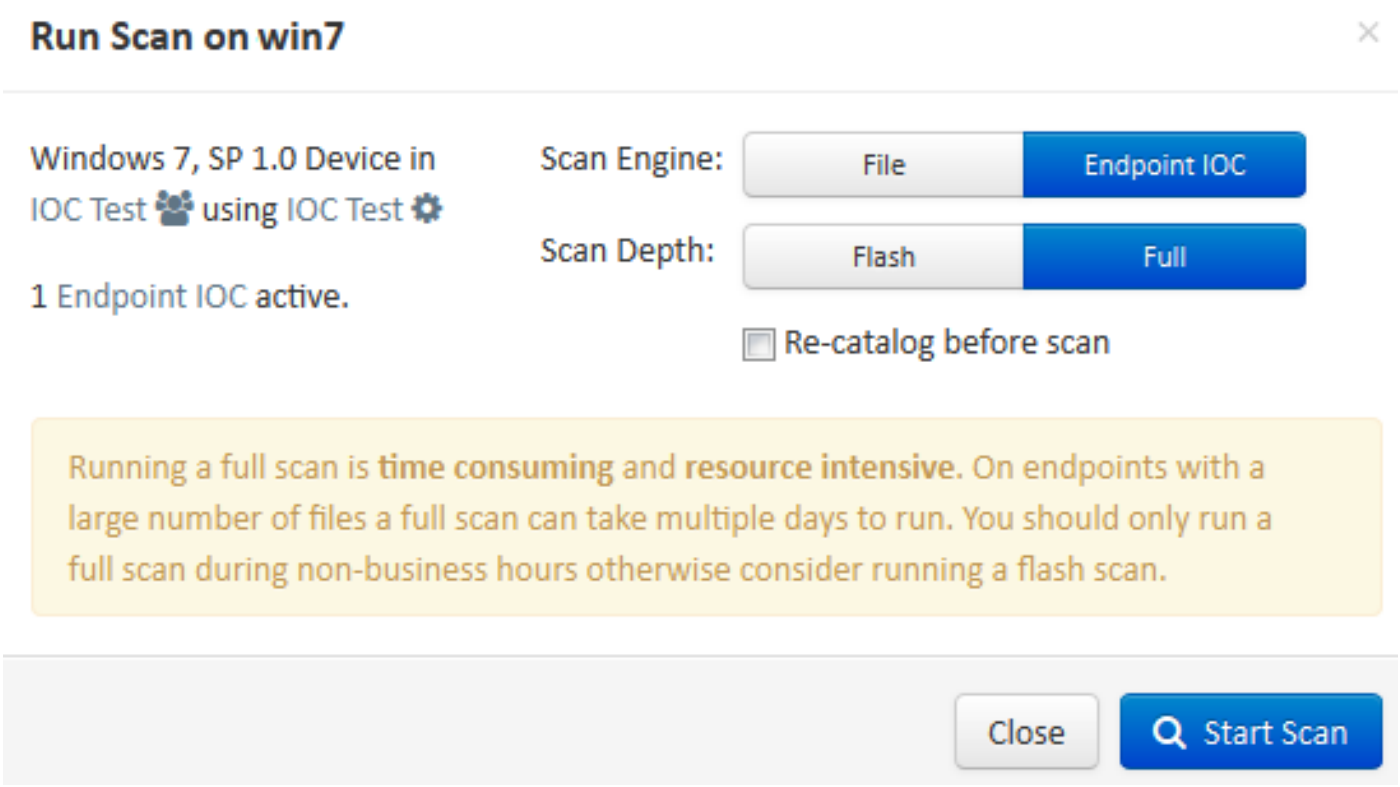
Iniciar un análisis

Después de cargar un archivo de firma, realice una exploración *completa*. El primer escaneo debe ser un escaneo completo porque debe generar un catálogo de metadatos para todo el equipo, que puede tardar entre 1 y 2 horas. Puede realizar un escaneo *flash* después de que el sistema esté catalogado a través de un escaneo completo.

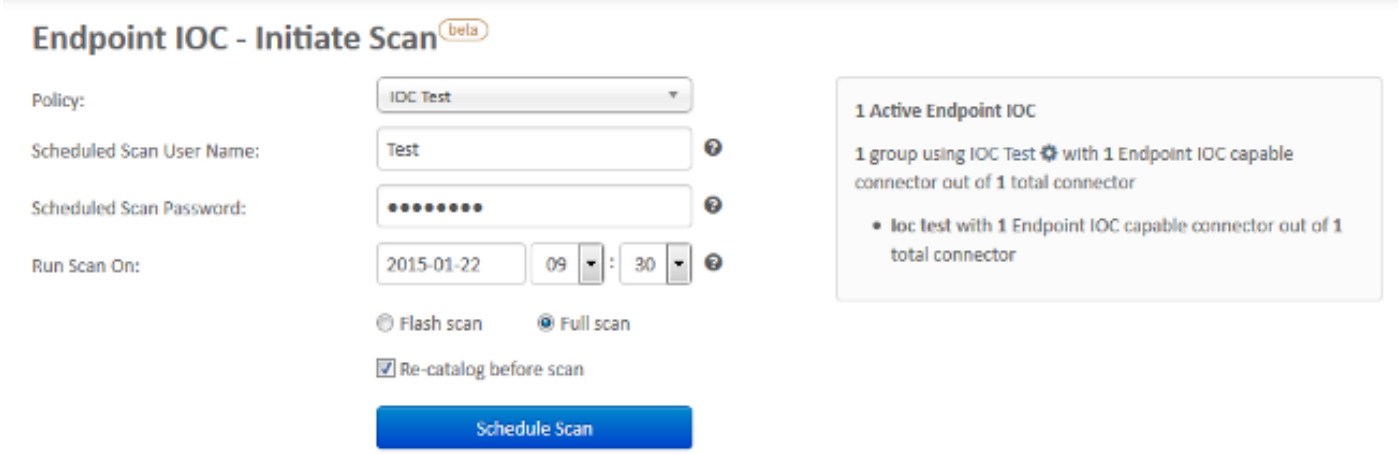
> **Nota:** El escaneo completo requiere un uso intensivo de la CPU. Cisco recomienda que no ejecute un escaneo completo en un PC mientras esté en uso. Si piensa utilizar la función con regularidad, puede realizar un escaneo completo una vez al mes para reconstruir el catálogo.

Hay dos métodos diferentes que puede utilizar para ejecutar un escaneo de IOC. El primer método consiste en realizar un análisis inmediato desde un evento o desde el panel. Esto se activa la próxima vez que un PC envíe un latido a la nube.

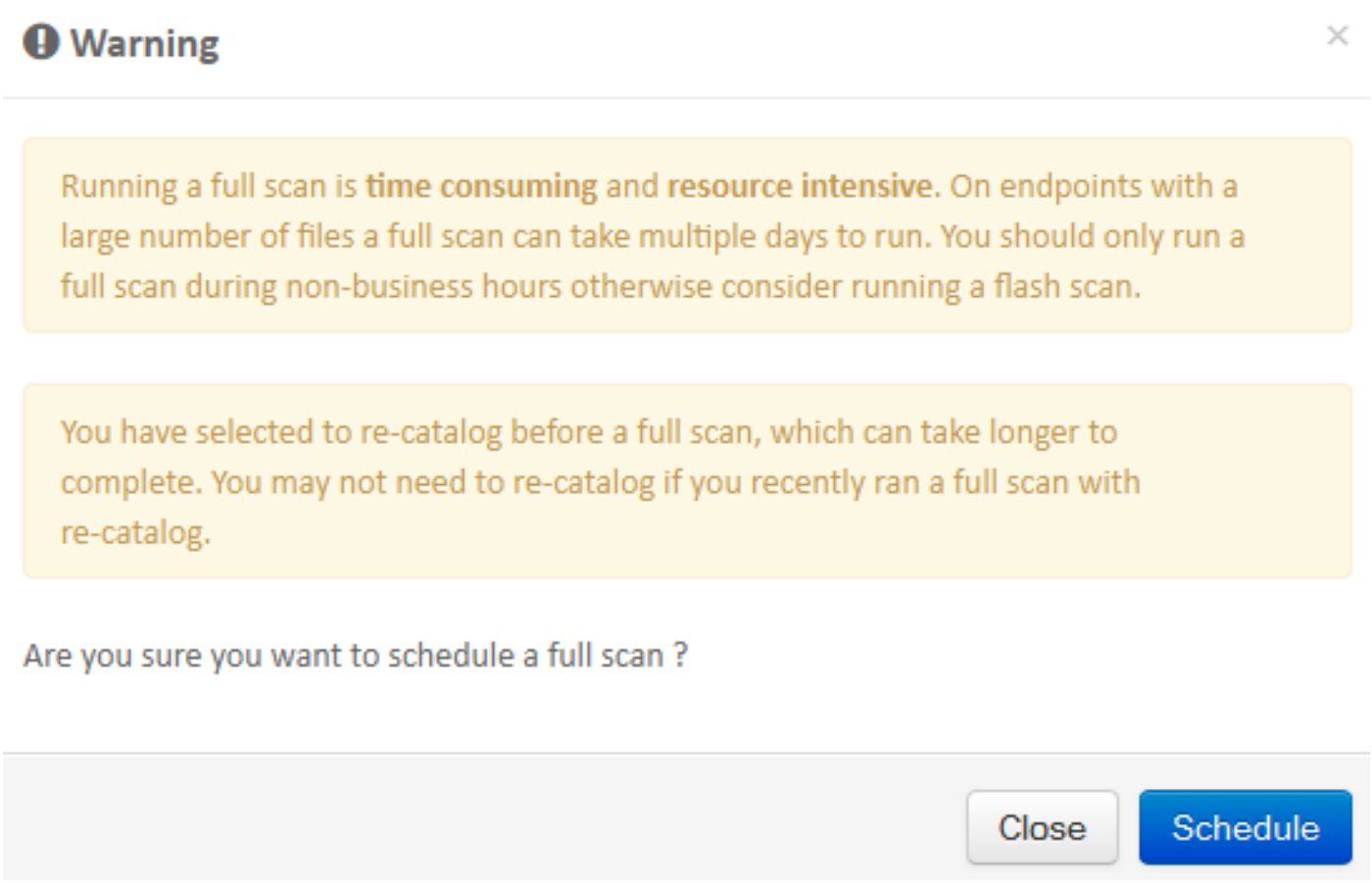
> **Nota:** Si es la primera vez que ejecuta el escaneo completo, no es necesario que compruebe la opción **Volver a catalogar antes del escaneo**.



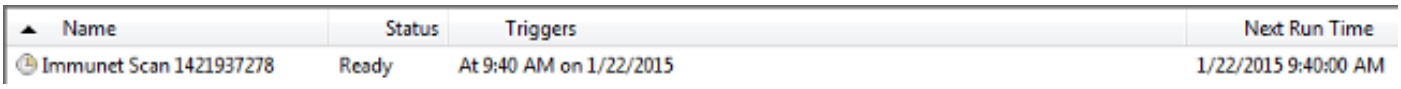
El segundo método consiste en crear un escaneo IOC de terminal programado desde el menú **Control de brotes** del panel. Esta opción puede ser ideal cuando desea realizar exploraciones durante horas fuera de las horas punta. Debe proporcionar las credenciales de una cuenta que tenga permiso en el equipo dado para crear tareas programadas y permitir el permiso de política **Iniciar sesión como** grupo de **lotes**.



Cuando programa un escaneo IOC de terminal, aparece este mensaje de advertencia:

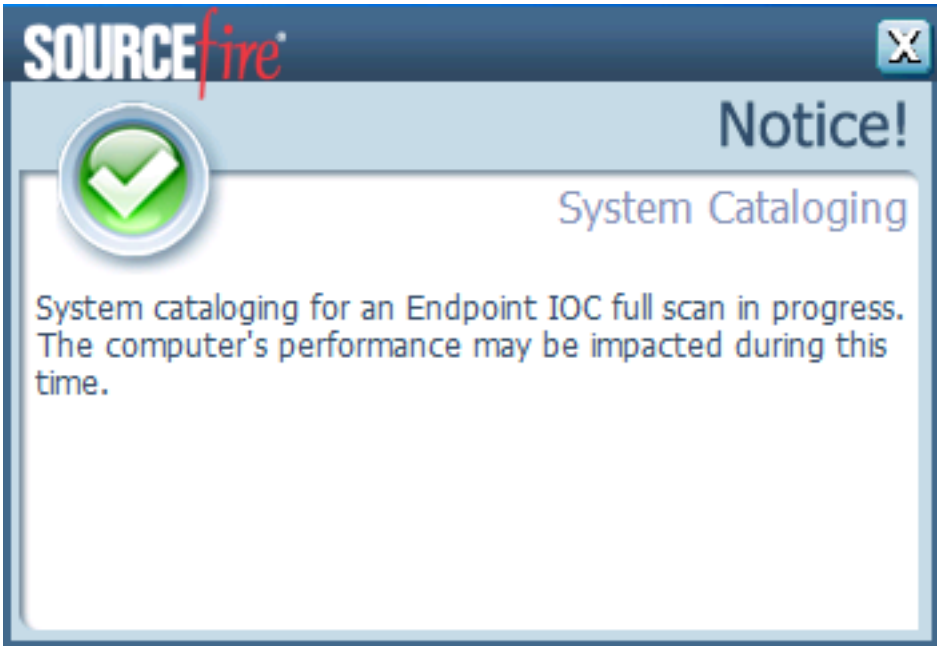


La próxima vez que el PC envíe un latido de corazón, y si las credenciales son válidas, debería ver un trabajo similar a este en Windows Task Scheduler:



Cuando se inicia el escaneo, aparece este mensaje:

> **Nota:** Si la GUI está configurada para ocultarse, entonces no verá el aviso **de catalogación del sistema**.



Cuando la exploración se complete, podrá ver el *resumen de detección de IOC de terminal*. Este ejemplo muestra una coincidencia para el archivo de firma **test.txt** IOC: