Effectuer des analyses IOC des terminaux avec AMP for Endpoints ou FireAMP

Contenu

Introduction

Ce document décrit comment créer un fichier de signature d'indication de compromission (IOC) via l'éditeur IOC Mandiant, comment le télécharger sur le tableau de bord Cisco FireAMP et comment lancer une analyse IOC de point d'extrémité.

Conditions préalables

Conditions requises

Cisco vous recommande de disposer d'au moins un gigaoctet d'espace libre avant d'essayer d'exécuter les analyses IOC des points d'extrémité.

Components Used

Les informations de ce document sont basées sur le scanner IOC des points d'extrémité, disponible dans les versions 4.0.2 et ultérieures du connecteur Windows Cisco FireAMP.

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.

Informations générales

La fonction de scanner IOC des points de terminaison est un puissant outil de réponse aux incidents qui est utilisé pour analyser les indicateurs de post-compromission sur plusieurs ordinateurs.

> **Note**: Bien que FireAMP prenne en charge les CIO avec le langage Mandiant, le logiciel Mandiant IOC Editor lui-même n'est pas développé ou pris en charge par Cisco. L'assistance Cisco ne dépanne pas les CIO créés par l'utilisateur ou par des tiers.

Fichiers de signature du CIO

Le fichier de signature du CIO est un schéma XML extensible pour la description des caractéristiques techniques qui identifient une menace connue, une méthodologie d'attaque ou toute autre preuve de compromission.

Vous pouvez importer des IOC de point de terminaison via la console à partir de fichiers OpenIOC écrits afin de déclencher des propriétés de fichier telles que le nom, la taille et le hachage, ainsi que d'autres attributs et propriétés système tels que les informations de processus, les services en cours d'exécution et les entrées du Registre Microsoft Windows. La syntaxe IOC peut être utilisée par les intervenants en cas d'incident afin de trouver des artefacts spécifiques ou dans le but d'utiliser la logique pour créer des détections sophistiquées et corrélées pour les familles de programmes malveillants.

Exécuter une analyse sur un fichier de signature IOC

Vous devez effectuer trois étapes pour exécuter une analyse sur un fichier de signature IOC :

1. Créez un fichier de signature IOC.
2. Téléchargez le fichier de signature du CIO.
3. Lancer une analyse.

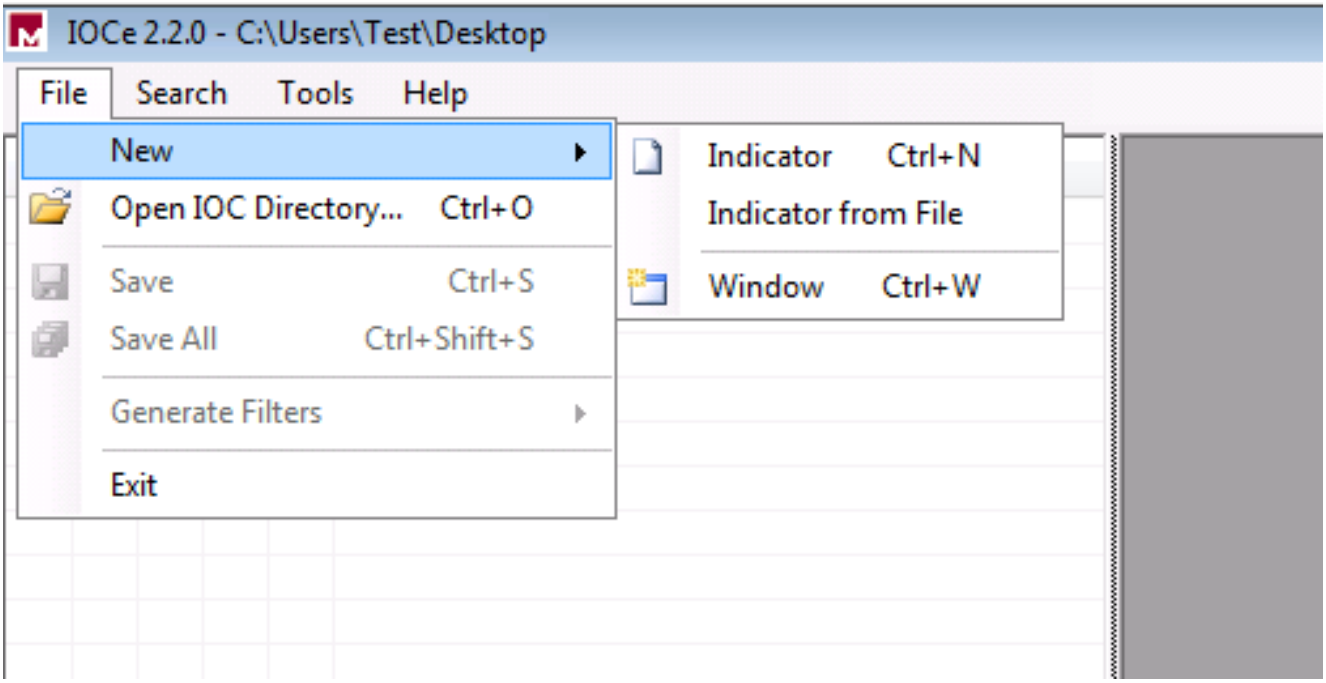
Ces étapes sont développées dans les sections suivantes.

Créer un fichier de signature IOC

> **Note**: Dans cet exemple, l'éditeur IOC Mandiant est utilisé afin de créer un fichier de signature IOC pour un fichier texte nommé **test.txt**.

Complétez ces étapes afin de créer un fichier de signature IOC :

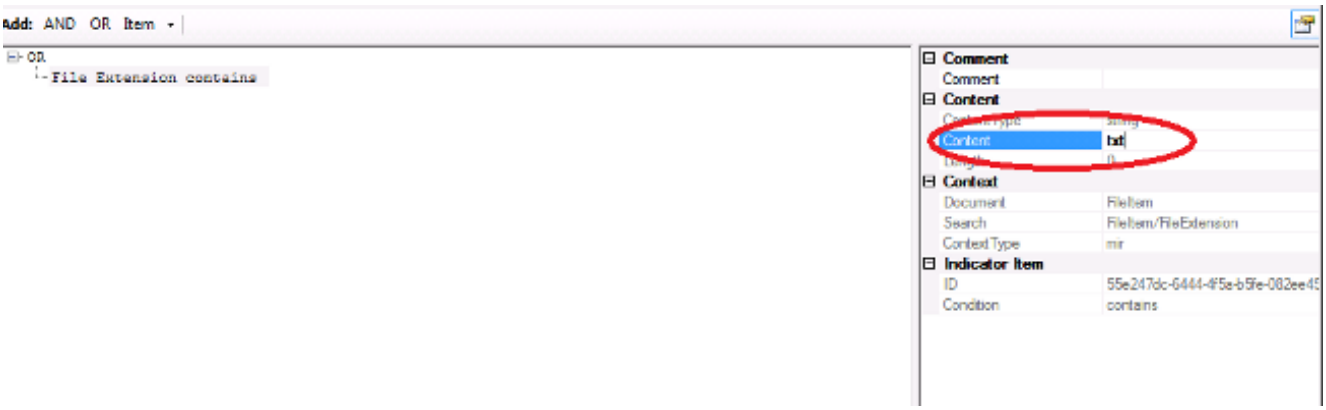
1. Ouvrez le **CIOe** et accédez à **Fichier > Nouveau > Indicateur**. Cet espace de travail vide vous permet de commencer à créer un CIO.



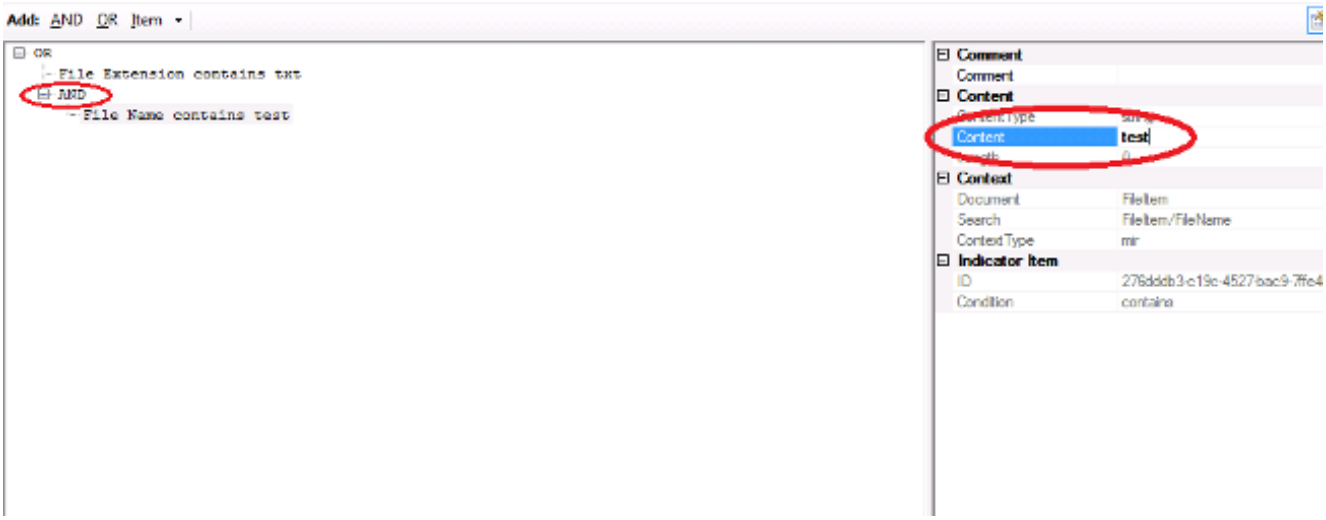
Note: Afin de créer un CIO pour quelque chose de spécifique, utilisez une logique binaire avec les propriétés. L'opérateur initial est un OU, qui est la base la plus simple à utiliser. Cela permet au CIO de fonctionner dans un premier temps, de sorte que vous n'êtes pas tenu de le modifier. Il est nécessaire qu'un fichier de signature du CIO ait au moins deux propriétés ou conditions pour pouvoir l'utiliser correctement dans une analyse.

2. Cliquez sur le menu déroulant **Éléments** afin d'ajouter des opérateurs. La première propriété que vous devez ajouter est **l'extension de fichier contient**. Recherchez la propriété dans le menu de l'arborescence des **éléments** et cliquez dessus.

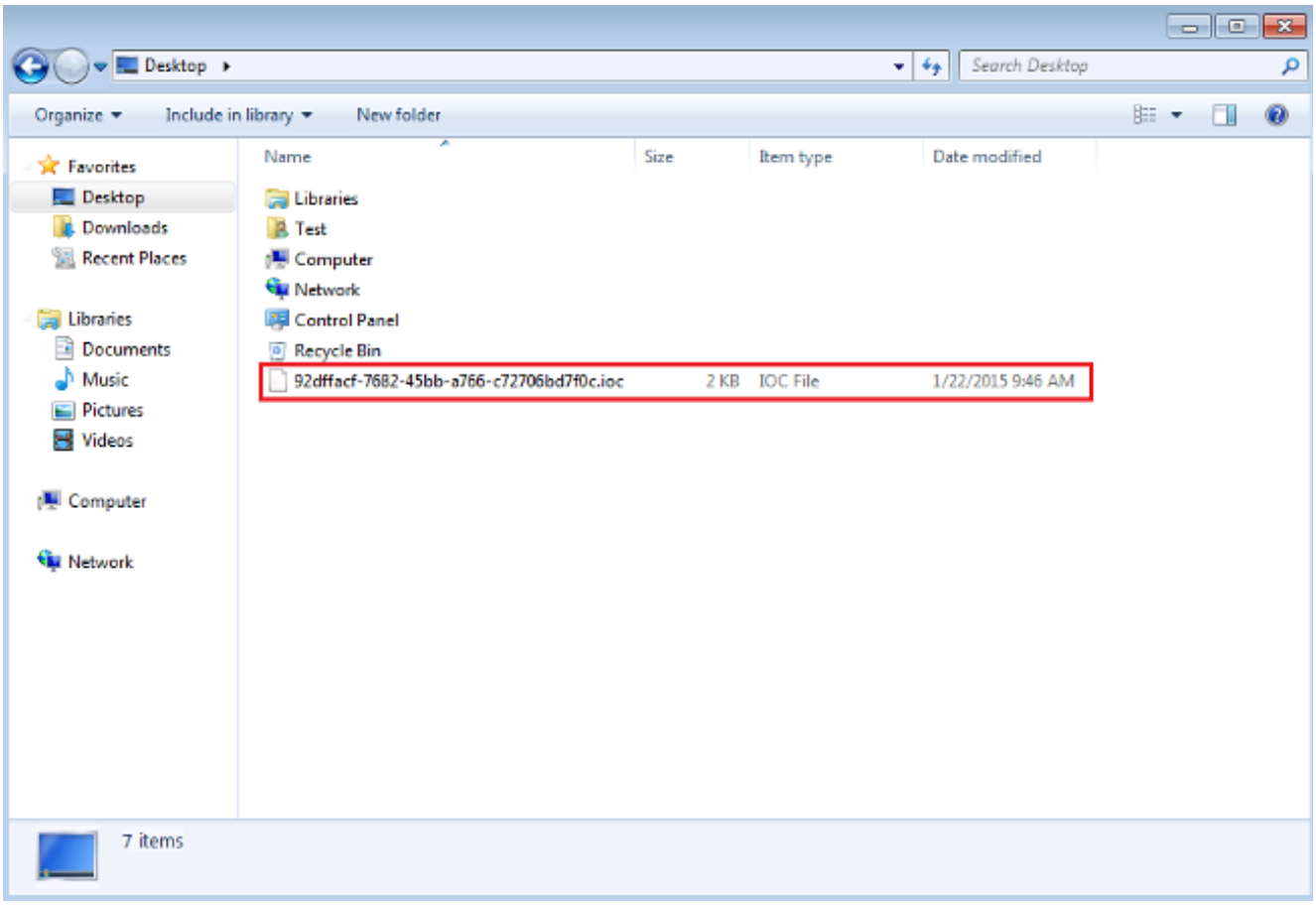
3. Après avoir ajouté une propriété, cliquez sur la petite icône située à l'extrême droite de l'écran afin d'ouvrir le volet Configuration. Dans ce volet, utilisez le champ **Contenu** afin de faire correspondre une extension de fichier. Par exemple, ajoutez **txt** afin de correspondre au fichier texte **test.txt** :



4. Vous devez maintenant ajouter un opérateur logique. Dans cet exemple, vous allez correspondre au fichier texte **test**. Afin de faire correspondre ceci, utilisez un opérateur *AND* et ajoutez la propriété suivante. Recherchez le nom du fichier et sélectionnez-le dans le menu de l'arborescence **Éléments**. Dans le volet Propriétés, ajoutez le nom du fichier à rechercher. Par exemple, ajoutez **test** dans le champ Contenu :



5. Comme aucune propriété supplémentaire n'est nécessaire pour ce simple IOC, vous pouvez maintenant enregistrer le fichier. Cliquez sur **Fichier > Enregistrer**, et un fichier de signature avec une extension **.ioc** est enregistré sur le système :



Télécharger un fichier de signature IOC

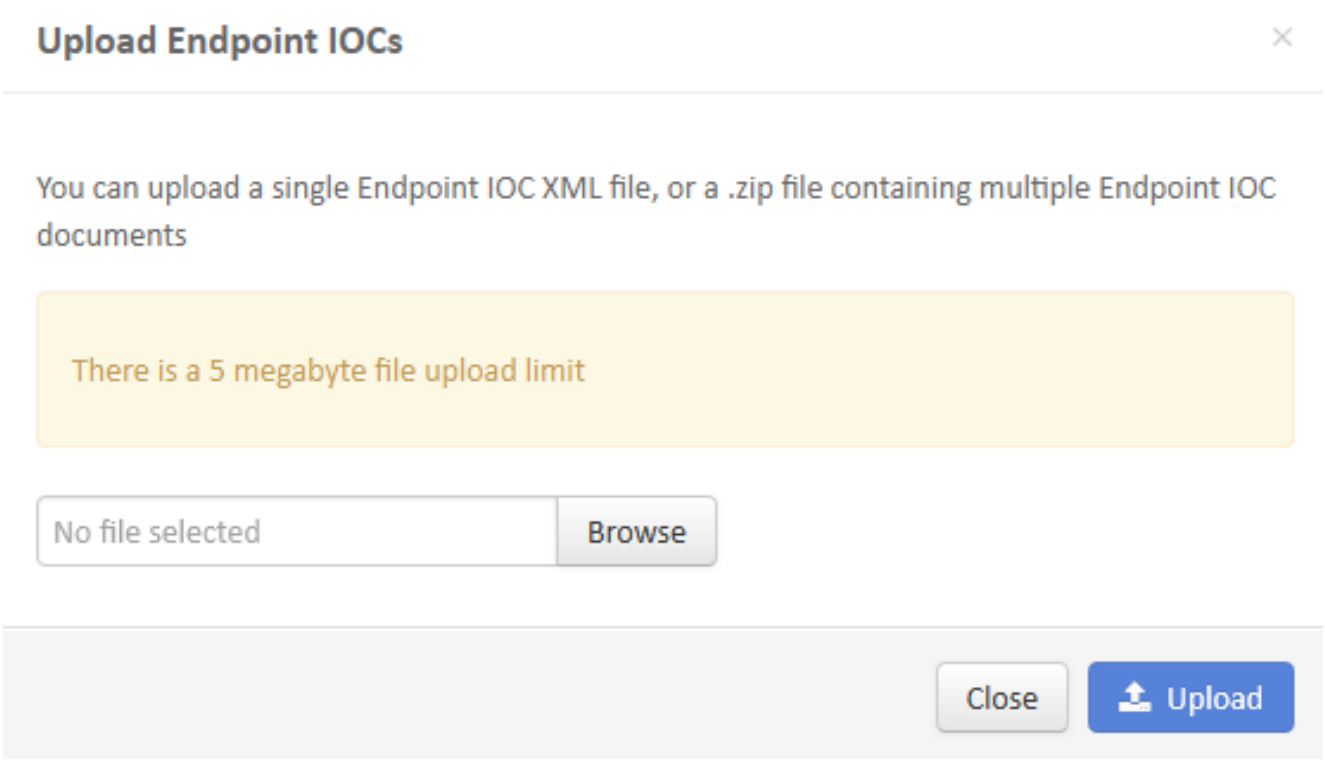
Pour effectuer une analyse, vous devez télécharger un fichier IOC sur le tableau de bord FireAMP. Vous pouvez utiliser un fichier de signature IOC, un fichier XML ou une archive zip contenant plusieurs fichiers IOC. Le tableau de bord décompresse et analyse le fichier avec les signatures IOC. Vous êtes averti si une syntaxe incorrecte ou une propriété non prise en charge est utilisée.

Astuce : Vous pouvez télécharger des fichiers d'une taille maximale de cinq mégaoctets.

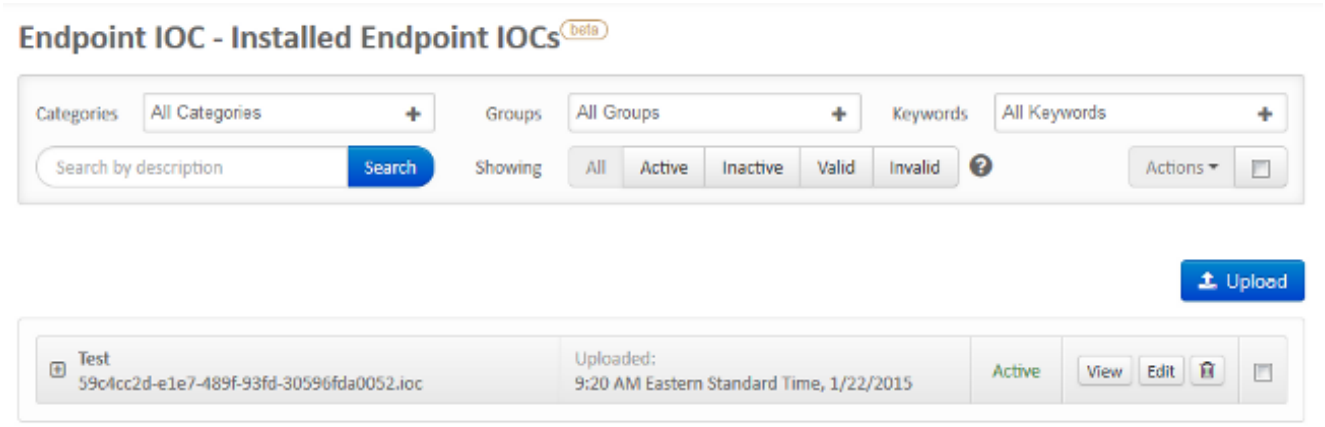
Complétez ces étapes afin de télécharger le fichier de signature IOC sur le tableau de bord FireAMP :

1. Connectez-vous à la console de cloud FireAMP et accédez à **Contrôle des attaques > IOC de terminal installé**.

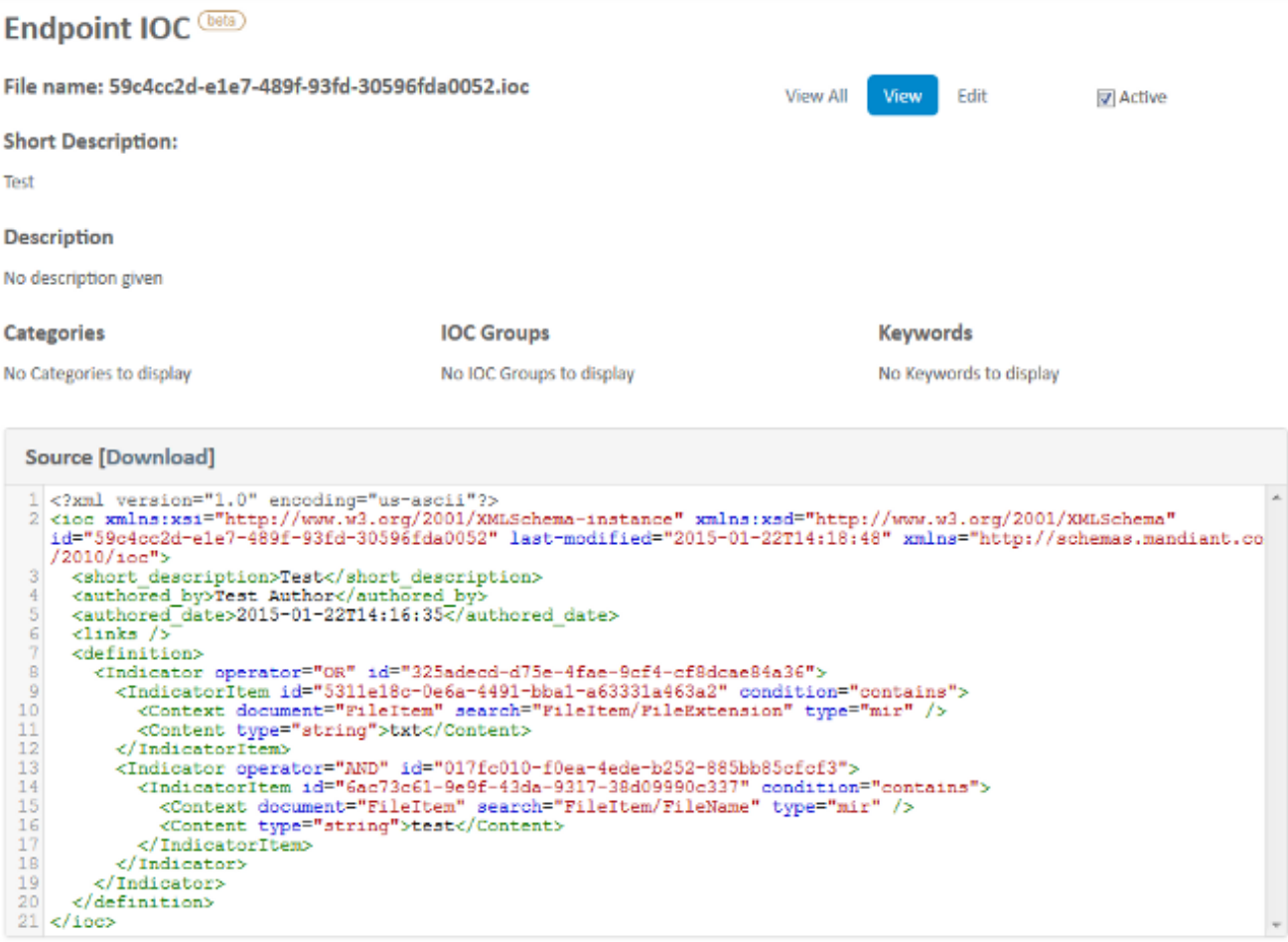
2. Cliquez sur **Upload**, et la fenêtre **Upload Endpoint IOCs** apparaît :



Une fois le fichier de signature du CIO téléchargé, la signature apparaît sur la liste :



3. Cliquez sur **Afficher** afin d'afficher les données XML réelles de la signature :



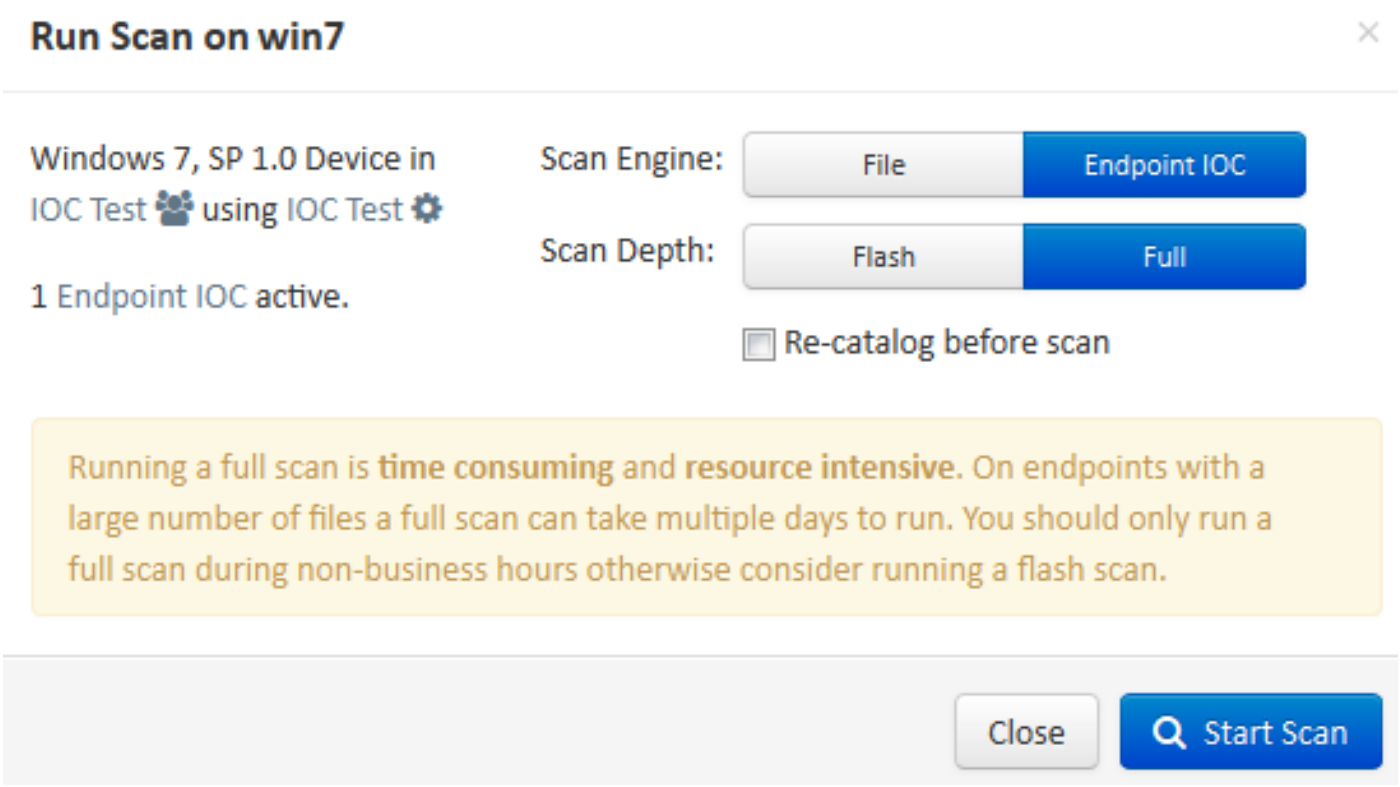
Lancer une analyse

Après avoir téléchargé un fichier de signature, effectuez une analyse *complète*. La première analyse doit être une analyse complète car elle doit créer un catalogue de métadonnées pour l'ensemble de l'ordinateur, ce qui peut prendre entre 1 et 2 heures. Vous pouvez effectuer une analyse *Flash* après avoir catalogué le système à l'aide d'une analyse complète.

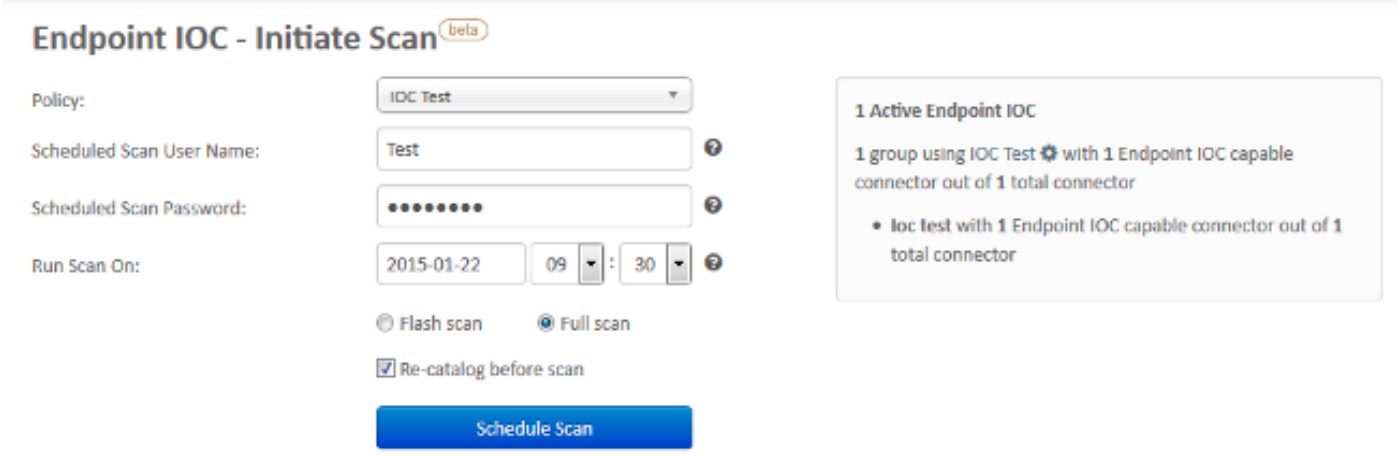
> **Note**: L'analyse complète est très gourmande en CPU. Cisco vous recommande de ne pas exécuter une analyse complète sur un PC lorsqu'il est utilisé. Si vous prévoyez d'utiliser régulièrement la fonctionnalité, vous pouvez effectuer une analyse complète une fois par mois afin de reconstruire le catalogue.

Vous pouvez utiliser deux méthodes différentes pour exécuter une analyse IOC. La première méthode consiste à effectuer une analyse immédiate à partir d'un événement ou du tableau de bord. Cela se déclenche la prochaine fois qu'un ordinateur envoie une pulsation au cloud.

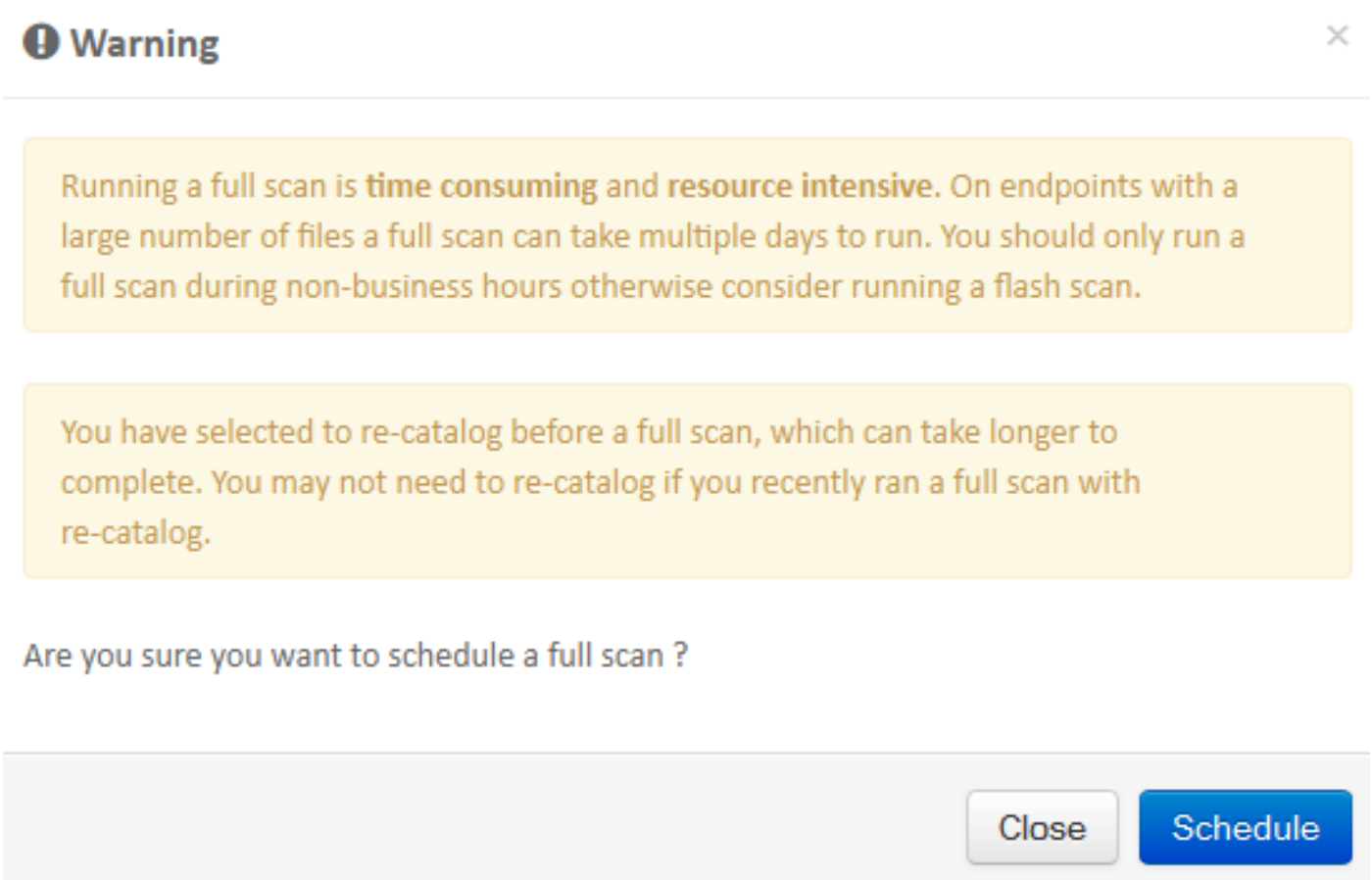
> **Note**: Si c'est la première fois que vous exécutez l'analyse complète, vous n'êtes pas tenu de vérifier l'option **Récataloguer avant l'analyse**.



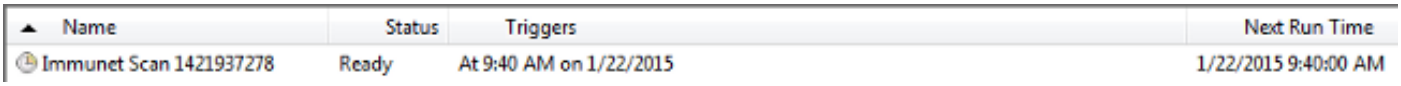
La deuxième méthode consiste à créer une analyse IOC de point de terminaison planifiée à partir du menu **Contrôle des attaques** du tableau de bord. Cette option peut être idéale lorsque vous souhaitez effectuer des analyses pendant les heures creuses. Vous devez fournir les informations d'identification d'un compte disposant d'une autorisation sur l'ordinateur donné afin de créer des tâches planifiées et d'autoriser l'autorisation de stratégie de groupe **Connexion en tant que lot**.



Lorsque vous planifiez une analyse IOC de point de terminaison, ce message d'avertissement apparaît :

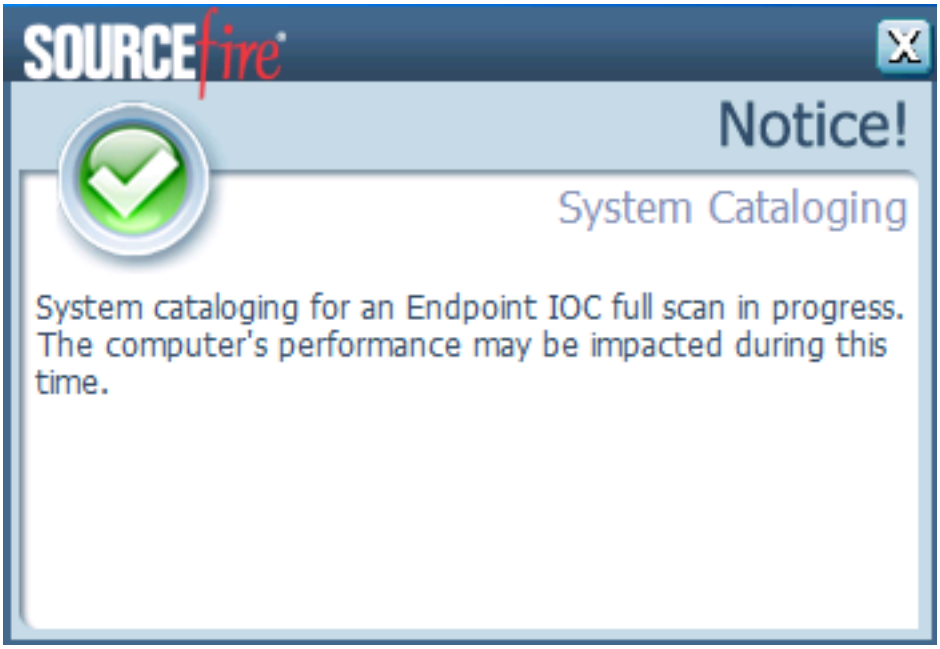


La prochaine fois que votre ordinateur envoie une pulsation et que vos informations d'identification sont valides, vous devriez voir un travail similaire à celui-ci dans le Planificateur de tâches Windows :



Au début de l'analyse, ce message s'affiche :

> **Note**: Si l'interface utilisateur graphique est configurée pour être masquée, l'avis **Catalogage système** ne s'affiche pas.



Une fois l'analyse terminée, vous pouvez afficher le *résumé de détection IOC du point de terminaison*. Cet exemple montre une correspondance pour le fichier de signature IOC **test.txt** :