Exécutez l'indication de point final des balayages de la compromission (COI) avec l'AMPÈRE pour des points finaux ou FireAMP

Contenu

Introduction

Ce document décrit comment créer une indication de fichier de signatures de la compromission (COI) par l'intermédiaire de l'éditeur COI de Mandiant, comment le télécharger au tableau de bord de Cisco FireAMP, et comment initier un COI de point final balayez.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez au moins un giga de l'espace lecteur libre avant que vous tentiez d'exécuter les balayages COI de point final.

[Composants utilisés](#)

Les informations dans ce document sont basées sur le module de balayage COI de point final, qui est disponible dans les versions 4.0.2 et ultérieures de connecteur de Cisco FireAMP Windows.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-

vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

La caractéristique de scanner COI de point final est un outil puissant de réponse d'incident qui est utilisé afin de balayer des indicateurs de POST-compromission à travers de plusieurs ordinateurs.

> Remarque: Bien que FireAMP prenne en charge l'iocs avec le langage de Mandiant, le logiciel d'éditeur COI de Mandiant lui-même n'est pas développé ou est pris en charge par Cisco. Cisco les prennent en charge ne dépanne pas créé par l'utilisateur ou la tierce partie iocs.

Fichiers de signatures COI

Le fichier de signatures COI est un schéma XML extensible pour la description des caractéristiques techniques qui identifient une menace connue, une méthodologie d'attaquant, ou d'autres preuves de compromission.

Vous pouvez importer le point final iocs par la console des fichiers basés sur OpenIOC qui sont écrits afin de déclencher sur des propriétés de fichier telles que le nom, la taille, et les informations parasites, aussi bien que d'autres attributs et propriétés de système telles que les informations sur le processus, des services courants, et des entrées dans le registre de Microsoft Windows. La syntaxe COI peut être utilisée par des responders d'incident afin de trouver les objets façonnés spécifiques ou afin d'employer la logique pour créer des détections sophistiquées et corrélées pour des familles de malware.

Exécutez un balayage sur un fichier de signatures COI

Il y a trois étapes que vous devez se terminer afin d'exécuter un balayage sur un fichier de signatures COI :

1. Créez un fichier de signatures COI.
2. Téléchargez le fichier de signatures COI.
3. Initiez un balayage.

Ces étapes sont développées au moment dans les sections qui suivent.

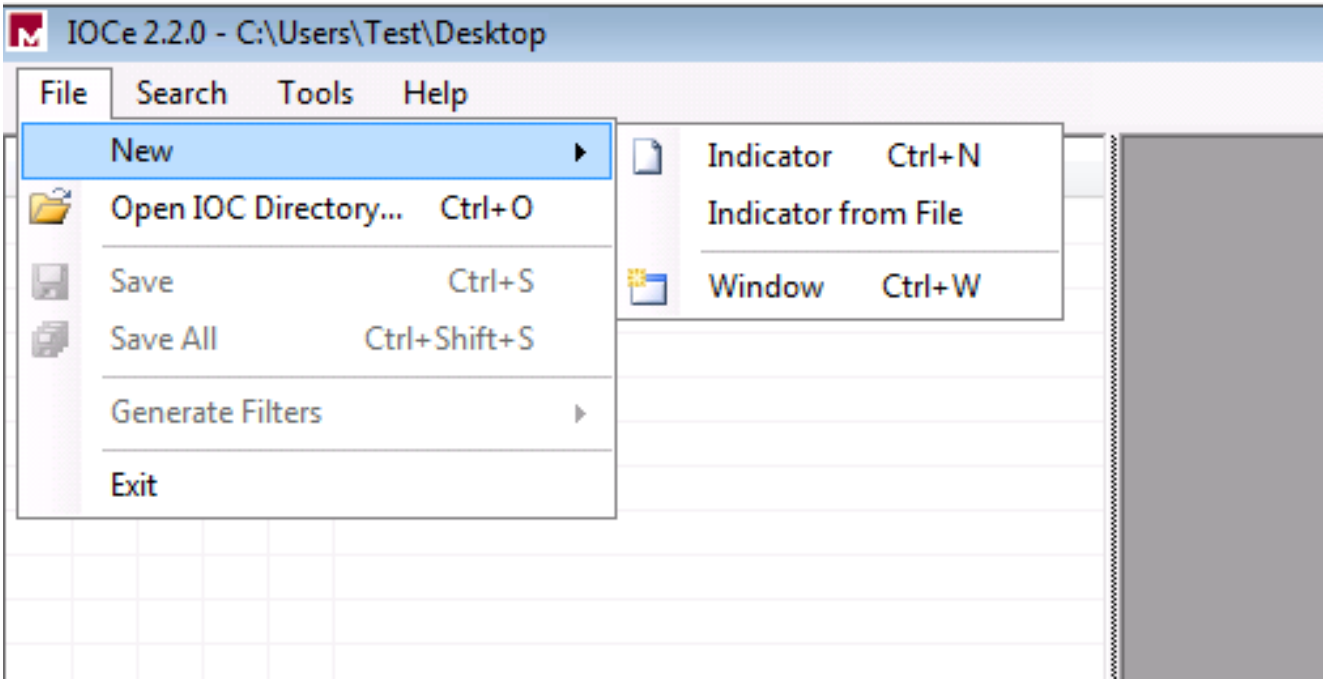
Créez un fichier de signatures COI

> Remarque: Dans cet exemple, l'éditeur COI de Mandiant est utilisé afin d'établir un fichier de signatures COI pour un fichier texte nommé **test.txt**.

Terminez-vous ces étapes afin de créer un fichier de signatures COI :

1. Ouvrez l'**IOCe** et naviguez **pour classer > nouveau > indicateur**. Ceci fournit un espace de

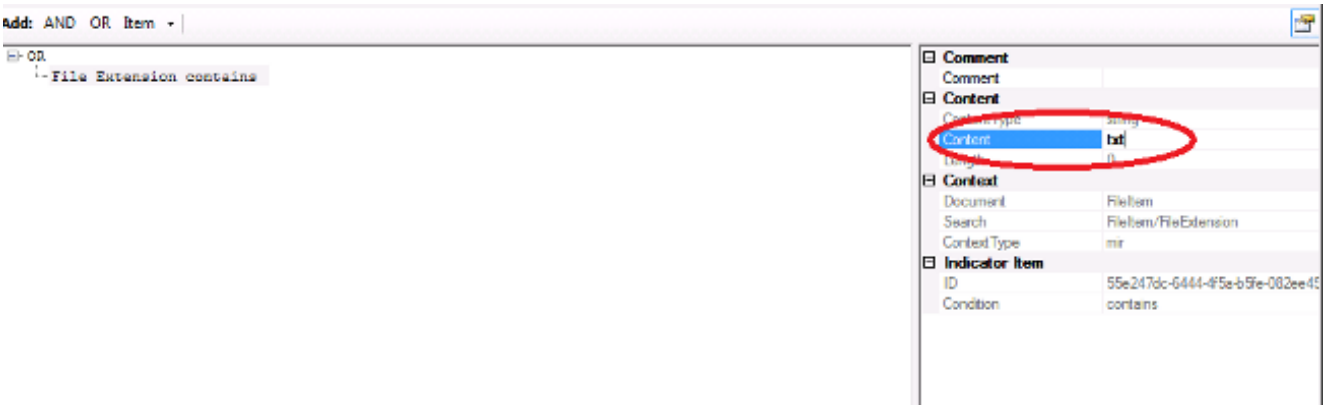
travail vide de sorte que vous puissiez commencer à construire un COI.



Remarque: Afin de créer un COI pour quelque chose spécifique, utilisez la logique binaire avec les propriétés. L'opérateur initial est dont OU, est la base la plus simple à fonctionner. Ceci permet à la fonction initiale du COI pour fonctionner, ainsi vous n'êtes pas requis de la changer. On l'exige qu'un fichier de signatures COI a au moins deux propriétés ou conditions afin de l'utiliser avec succès dans un balayage.

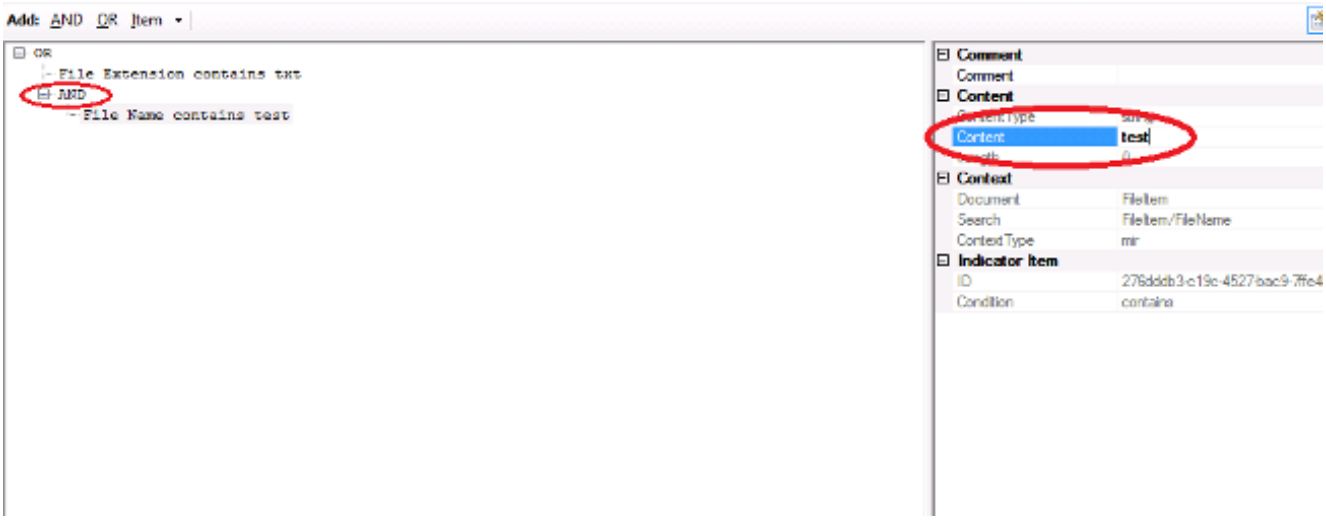
2. Cliquez sur le menu déroulant d'**éléments** afin d'ajouter des opérateurs. La première propriété que vous devriez ajouter est **extension de fichier contient**. Trouvez la propriété dans le menu d'arborescence d'**éléments** et cliquez sur-la.

3. Après que vous ajoutiez une propriété, cliquez sur la petite icône du côté droit le côté d'extrême droite de l'écran afin d'ouvrir le volet de configuration. Dans ce volet, employez le champ **satisfait** afin d'apparier une extension de fichier. Par exemple, ajoutez le **txt** afin de sélectionner le fichier texte de **test.txt** :

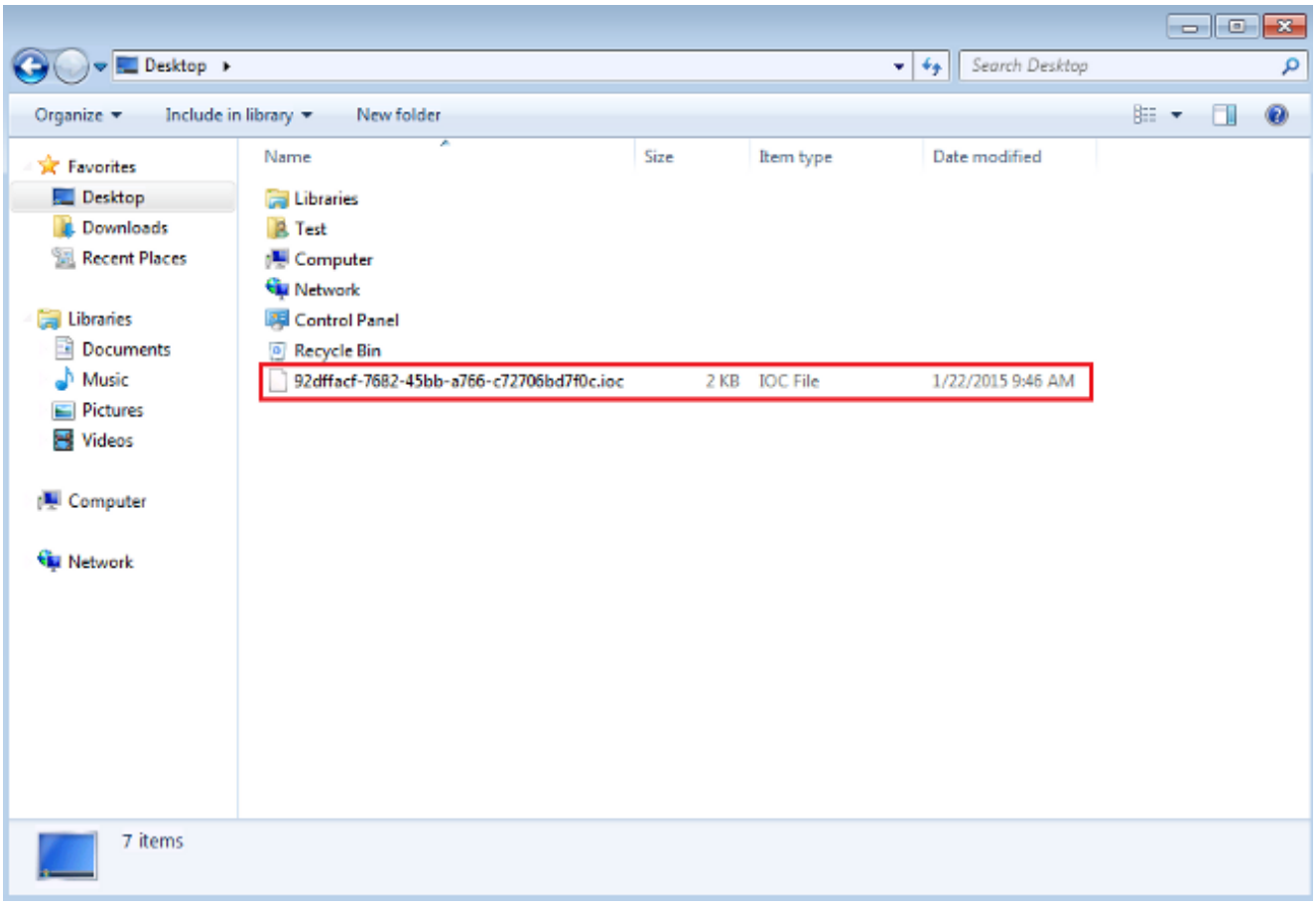


4. Vous devez maintenant ajouter un opérateur de logique. Dans cet exemple, vous sélectionnerez le fichier de **texte d'essai**. Afin d'apparier ceci, utilisez *ET l'*opérateur et ajoutez la prochaine propriété. Localisez le nom du fichier et sélectionnez-le du menu d'arborescence d'**éléments**. Dans le volet de Properties, ajoutez le nom du fichier que vous

voulez pour le trouver. Par exemple, ajoutez le **test** dans le domaine satisfait :



5. Puisqu'aucune propriété supplémentaire n'est nécessaire pour ce COI simple, vous pouvez maintenant sauvegarder le fichier. **Le fichier > la sauvegarde de** clic, et un fichier de signatures avec une extension **.ioc** est enregistré sur le système :



Téléchargez un fichier de signatures COI

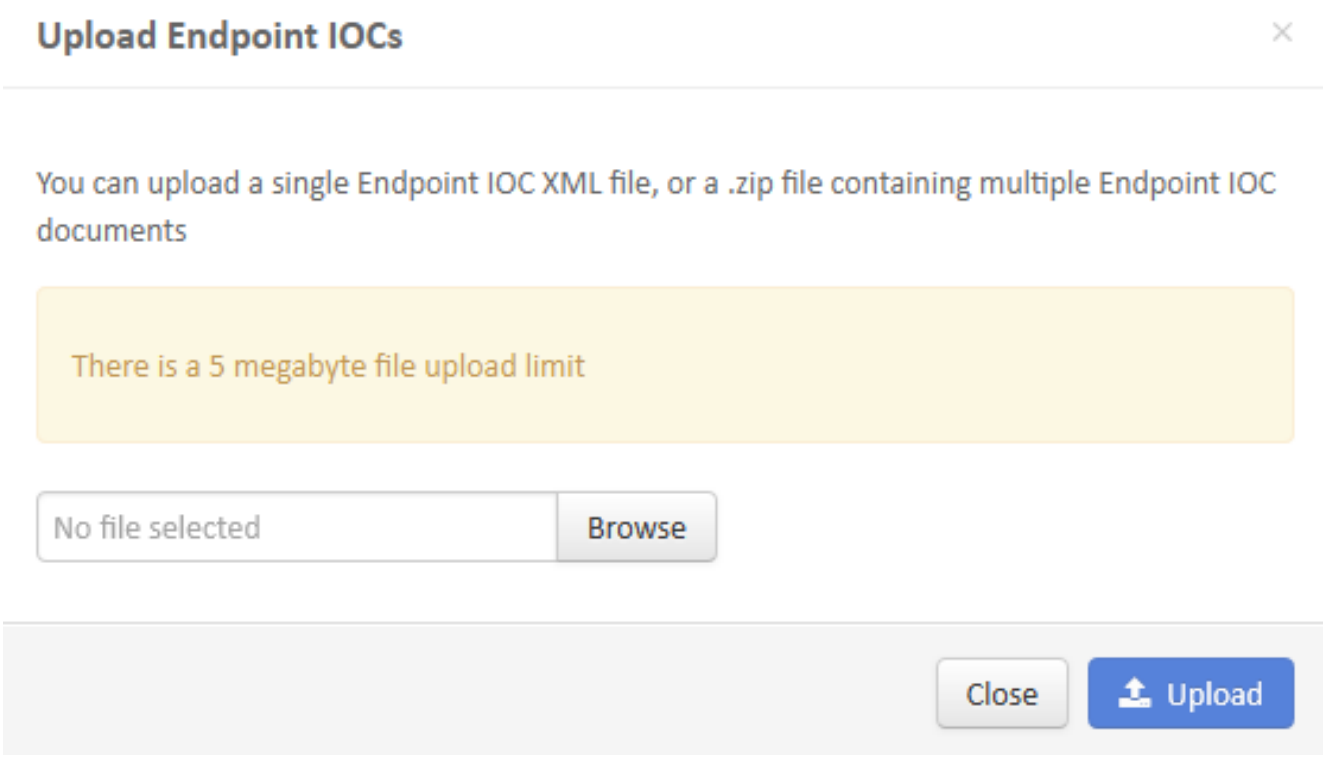
Afin d'exécuter un balayage, vous devez télécharger un COI classez au tableau de bord de FireAMP. Vous pouvez utiliser un fichier de signatures COI, un fichier XML, ou des archives de zip qui contiennent de plusieurs fichiers COI. Le tableau de bord décompresse et analyse le fichier avec les signatures COI. On vous annonce si une syntaxe incorrecte ou une propriété non vérifiée est utilisée.

Conseil : Vous pouvez télécharger les fichiers qui sont jusqu'à cinq mégaoctets dans la taille.

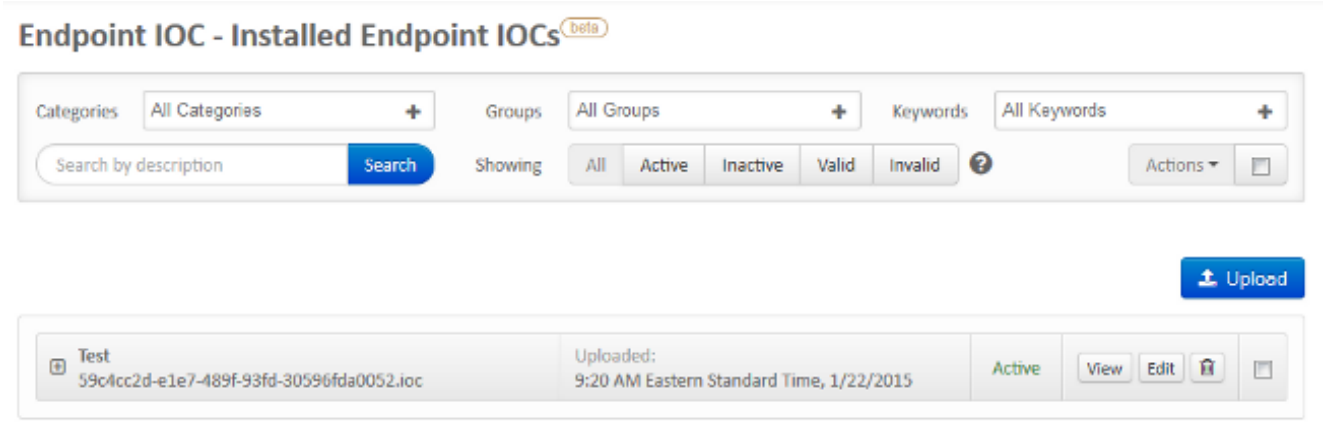
Terminez-vous ces étapes afin de télécharger le fichier de signatures COI au tableau de bord de FireAMP :

1. Connectez-vous dans la console de nuage de FireAMP et naviguez vers le **contrôle d'épidémie > COI installé de point final**.

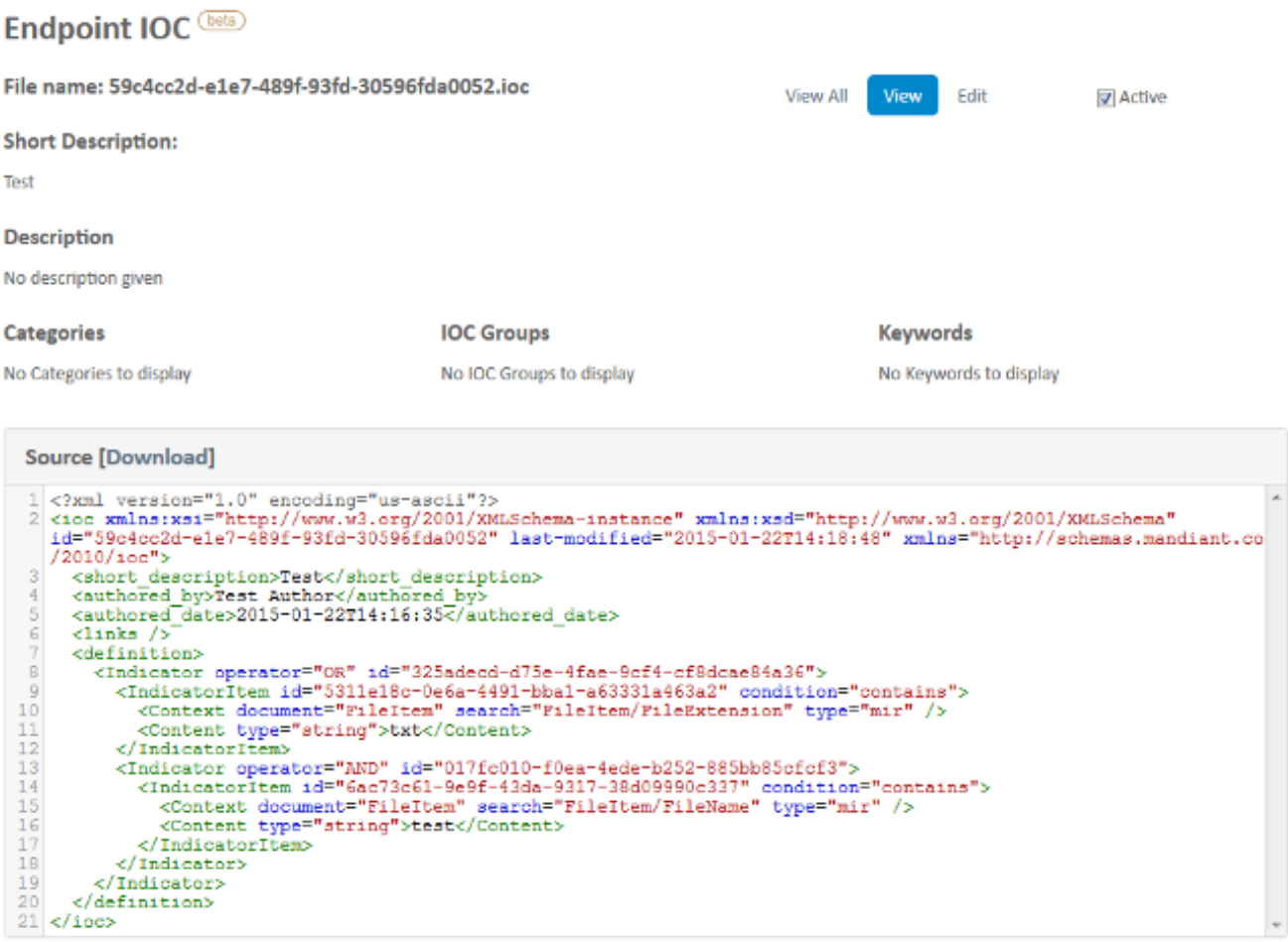
2. Cliquez sur Upload, et la fenêtre du **point final iocs de téléchargement** apparaît :



Après qu'un fichier de signatures COI soit téléchargé avec succès, la signature apparaît sur la liste :



3. Cliquez sur la **vue** afin de visualiser les données XML réelles de la signature :



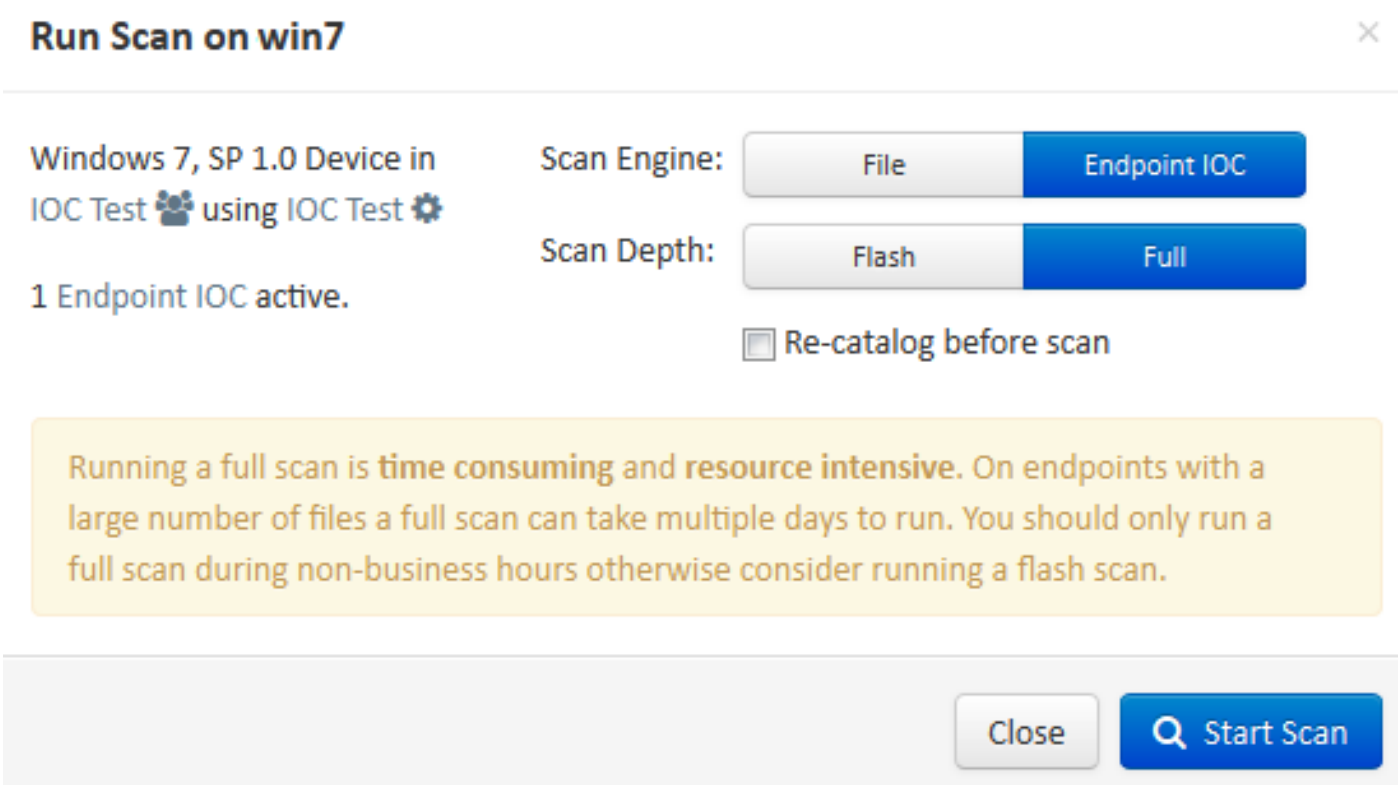
Initiez un balayage

Après que vous téléchargiez un fichier de signatures, exécutez un *plein* balayage. Le premier balayage doit être un plein balayage parce qu'il doit construire un catalogue des métadonnées pour l'ordinateur entier, qui peut prendre 1 – 2 heures. Vous pouvez exécuter un balayage *instantané* après que le système soit catalogué par un plein balayage.

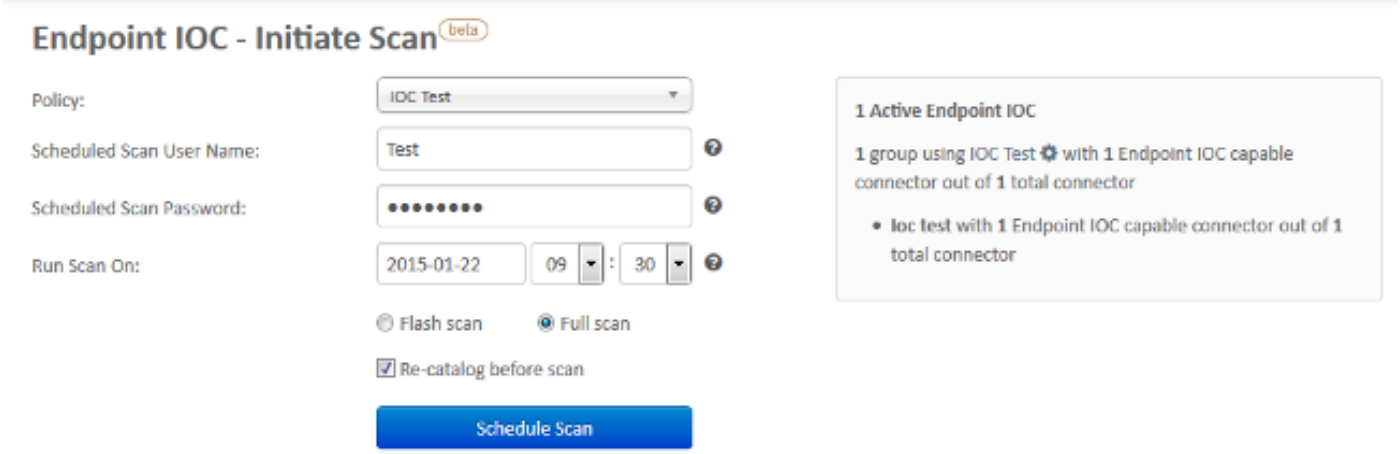
> Remarque: Le plein balayage est très CPU intensive. Cisco recommande que vous n'exécutiez pas un plein balayage sur un PC tandis qu'il est en service. Si vous prévoyez d'utiliser la caractéristique régulièrement, vous pouvez exécuter un plein balayage une fois par mois afin de reconstruire le catalogue.

Il y a deux différentes méthodes que vous pouvez employer afin de diriger un COI balayez. La première méthode est d'exécuter un balayage immédiat d'un événement ou du tableau de bord. Ceci est déclenché la prochaine fois qu'un PC envoie à une pulsation au nuage.

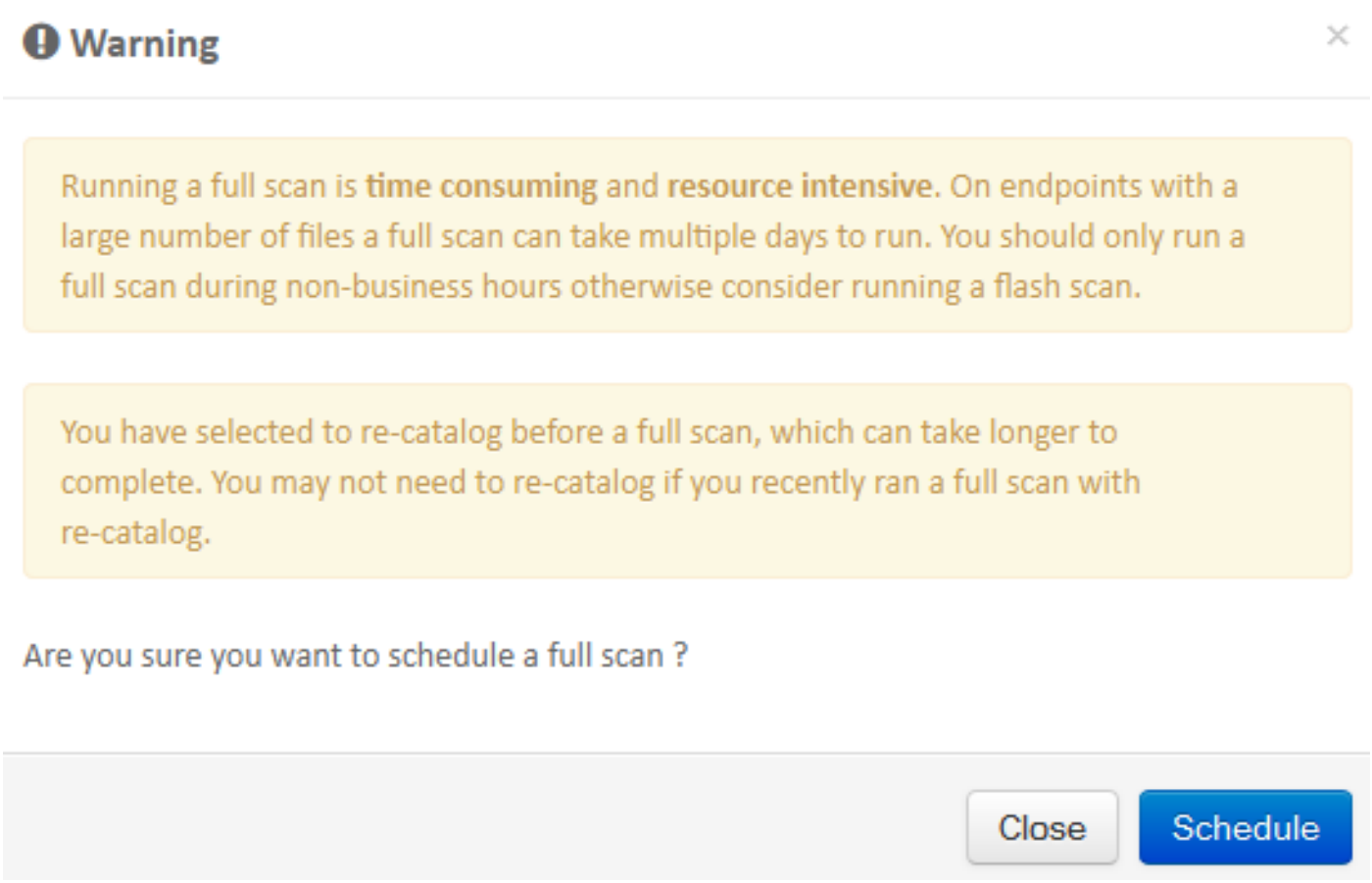
> Remarque: Si c'est la première fois que vous exécutez le plein balayage, vous n'êtes pas requis de vérifier le **recataloguage avant l'**option de **balayage**.



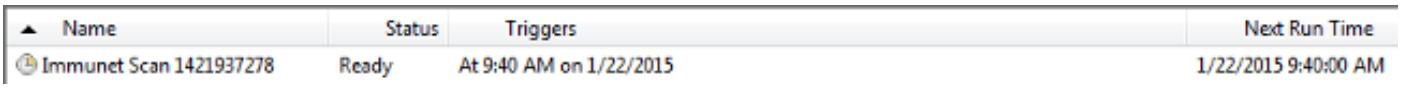
La deuxième méthode est de créer un COI programmé de point final balayent du menu de **contrôle d'épidémie du** tableau de bord. Cette option pourrait être idéale quand vous désirez exécuter des balayages pendant des heures creuses. Vous devez fournir les qualifications d'un compte qui a l'autorisation sur l'ordinateur donné afin de créer des tâches programmées et permettre le **login en tant qu'**autorisation de stratégie de groupe **en lots**.



Quand vous programmez un balayage COI de point final, ce message d'avertissement apparaît :



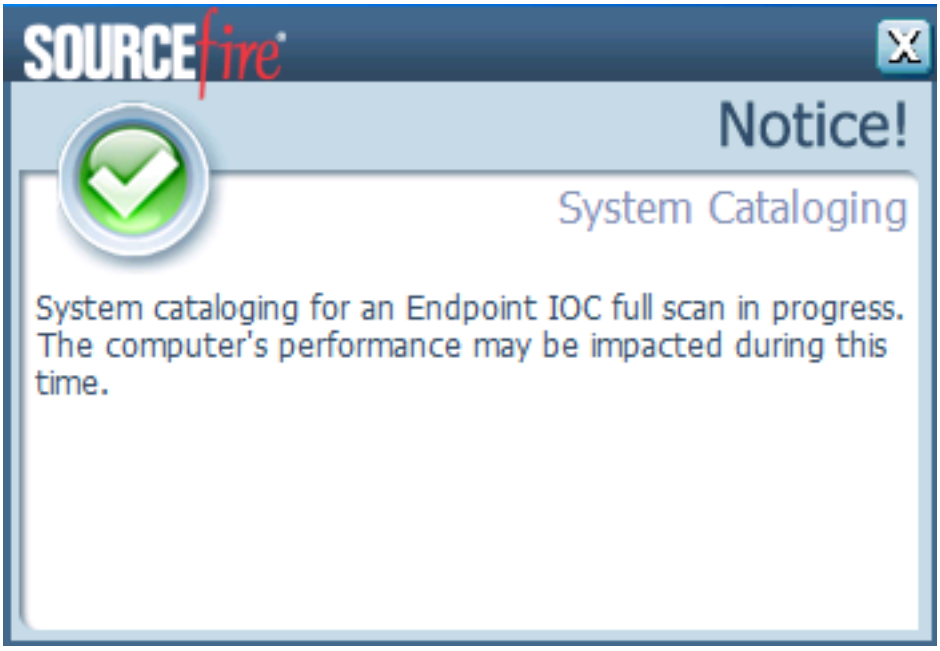
La prochaine fois que ce votre PC envoie une pulsation, et si vos qualifications sont valides, vous devriez voir un travail semblable à ceci dans le programmateur de tâche de Windows :



Name	Status	Triggers	Next Run Time
Immunet Scan 1421937278	Ready	At 9:40 AM on 1/22/2015	1/22/2015 9:40:00 AM

Quand le balayage commence, ce message apparaît :

> Remarque: Si le GUI est configuré pour être masqué, alors vous ne voyez pas l'avis **cataloguant de système**.



Quand le balayage est complet, vous pouvez visualiser le *COI de point final analysez le résumé de détection*. Cet exemple affiche une correspondance pour le fichier de signatures COI de **test.txt** :