Führen Sie Prüfungen zur Indication of Compromise (IOC) mit AMP für Endgeräte oder FireAMP durch.

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie eine Signaturdatei für die Indications of Compromise (IOC) über den Verwaltungs-IOC-Editor erstellen, wie Sie sie in das Cisco FireAMP-Dashboard hochladen und eine Endpunkt-IOC-Prüfung initiieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über mindestens ein Gigabyte freien Festplattenspeicherplatz verfügen, bevor Sie versuchen, die IOC-Prüfungen für Endgeräte durchzuführen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Endpunkt-IOC-Scanner, der in Cisco FireAMP Windows Connector Version 4.0.2 und höher verfügbar ist.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie

die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Die Endpunkt-IOC-Scannerfunktion ist ein leistungsstarkes Incident Response Tool, das zum Scannen von Indicators of Compromise auf mehreren Computern verwendet wird.

> **Hinweis**: Obwohl FireAMP IOCs mit der Sprache Mandiant unterstützt, wird die Mandiant IOC Editor-Software selbst nicht von Cisco entwickelt oder unterstützt. Der Cisco Support behebt keine Fehler bei von Benutzern oder Drittanbietern erstellten IOCs.

IOC-Signaturdateien

Die IOC-Signaturdatei ist ein erweiterbares XML-Schema für die Beschreibung technischer Merkmale, die eine bekannte Bedrohung, eine Angreifermethodik oder andere Anzeichen für eine Kompromittierung identifizieren.

Sie können Endpunkt-IOCs über die Konsole aus OpenIOC-basierten Dateien importieren, die geschrieben wurden, um Dateieigenschaften wie Name, Größe und Hash sowie andere Attribute und Systemeigenschaften wie Prozessinformationen, ausgeführte Dienste und Microsoft Windows-Registrierungseinträge auszulösen. Die IOC-Syntax kann von Incident Response Teams verwendet werden, um bestimmte Artefakte zu finden oder um Logik zu verwenden, um komplexe, korrelierte Erkennungen für Malware-Familien zu erstellen.

Führen Sie eine Prüfung auf einer IOC-Signaturdatei durch.

Sie müssen drei Schritte ausführen, um eine Prüfung auf einer IOC-Signaturdatei durchzuführen:

1. Erstellen Sie eine IOC-Signaturdatei.
2. Laden Sie die IOC-Signaturdatei hoch.
3. Starten Sie eine Prüfung.

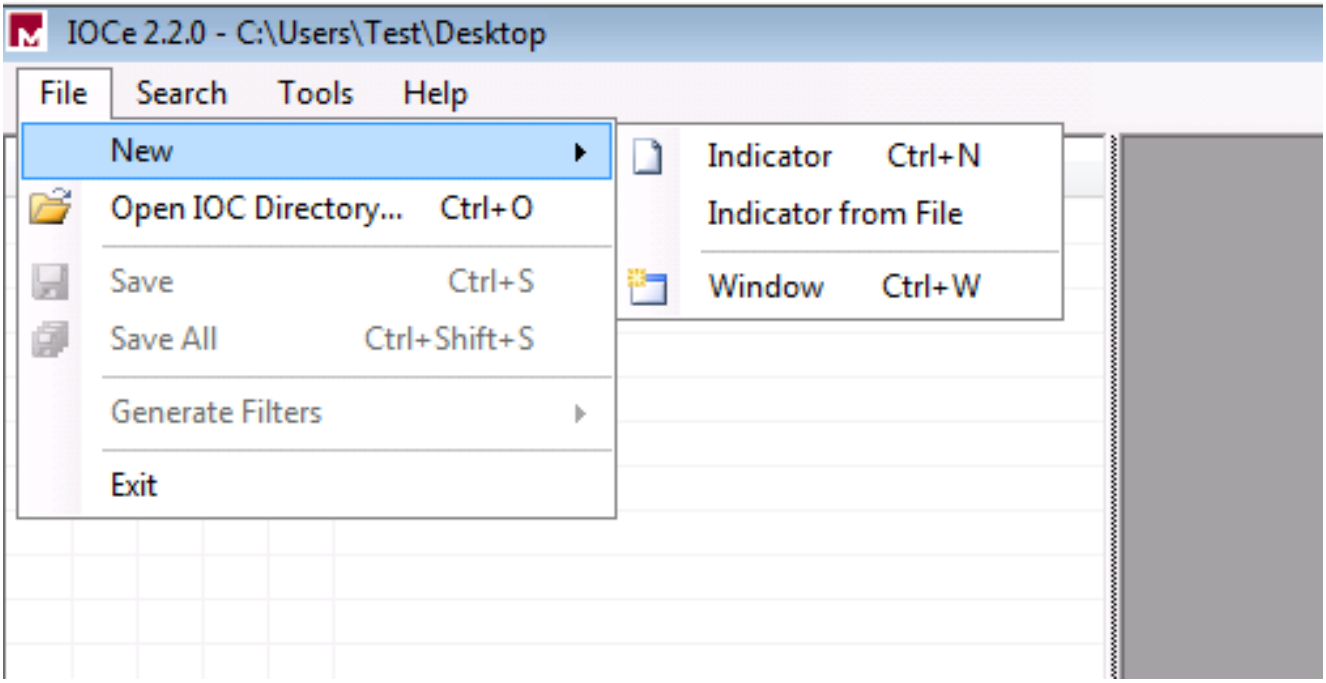
Diese Schritte werden in den folgenden Abschnitten erläutert.

Erstellen einer IOC-Signaturdatei

> **Hinweis**: In diesem Beispiel wird der verwaltete IOC-Editor verwendet, um eine IOC-Signaturdatei für eine Textdatei mit dem Namen **test.txt** zu erstellen.

Gehen Sie wie folgt vor, um eine IOC-Signaturdatei zu erstellen:

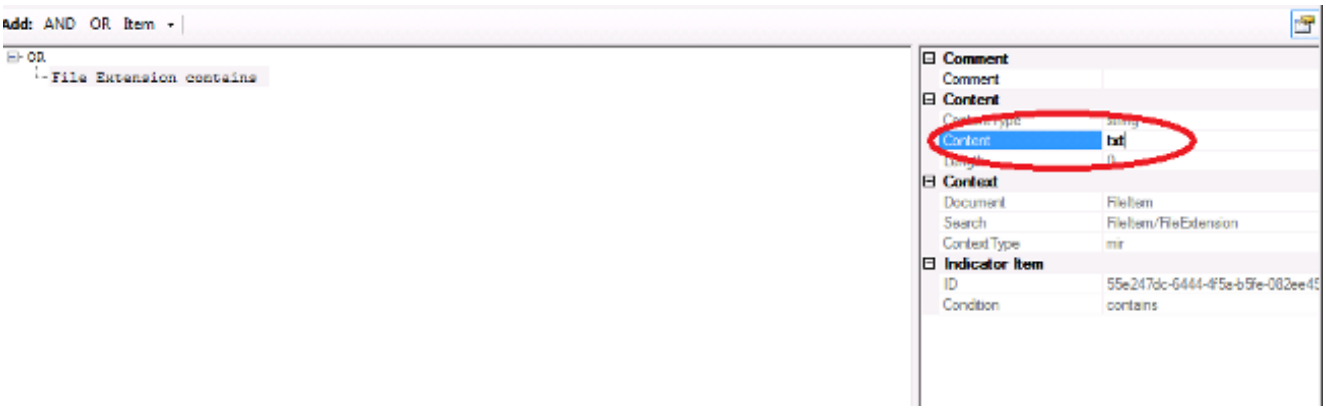
1. Öffnen Sie den **IOCe**, und navigieren Sie zu **Datei > Neu > Anzeige**. Dadurch wird ein leerer Arbeitsbereich bereitgestellt, sodass Sie mit der Erstellung eines IOC beginnen können.



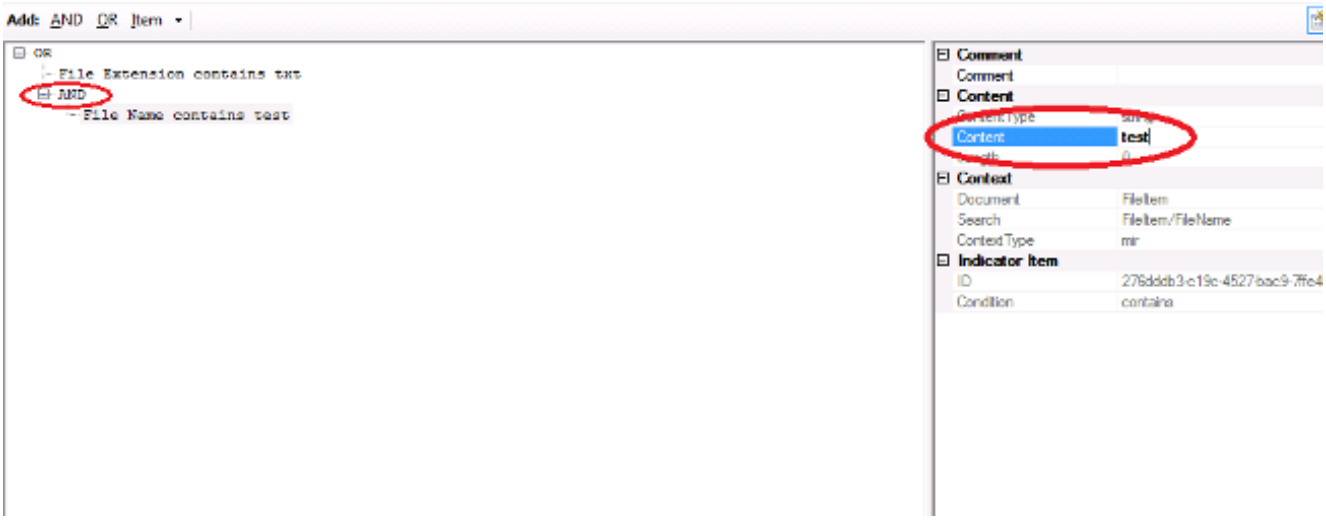
Hinweis: Um einen IOC für etwas Bestimmtes zu erstellen, verwenden Sie binäre Logik mit den Eigenschaften. Der erste Operator ist OR, also die einfachste Ausgangsbasis für die Arbeit. Dadurch kann die anfängliche IOC-Funktion funktionieren, sodass Sie sie nicht ändern müssen. Eine IOC-Signaturdatei muss mindestens zwei Eigenschaften oder Bedingungen aufweisen, um sie in einer Prüfung erfolgreich verwenden zu können.

2. Klicken Sie auf das Dropdown-Menü **Artikel**, um Operatoren hinzuzufügen. Die erste Eigenschaft, die Sie hinzufügen sollten, ist **File Extension enthält**. Suchen Sie die Eigenschaft im Strukturmenü **Artikel**, und klicken Sie darauf.

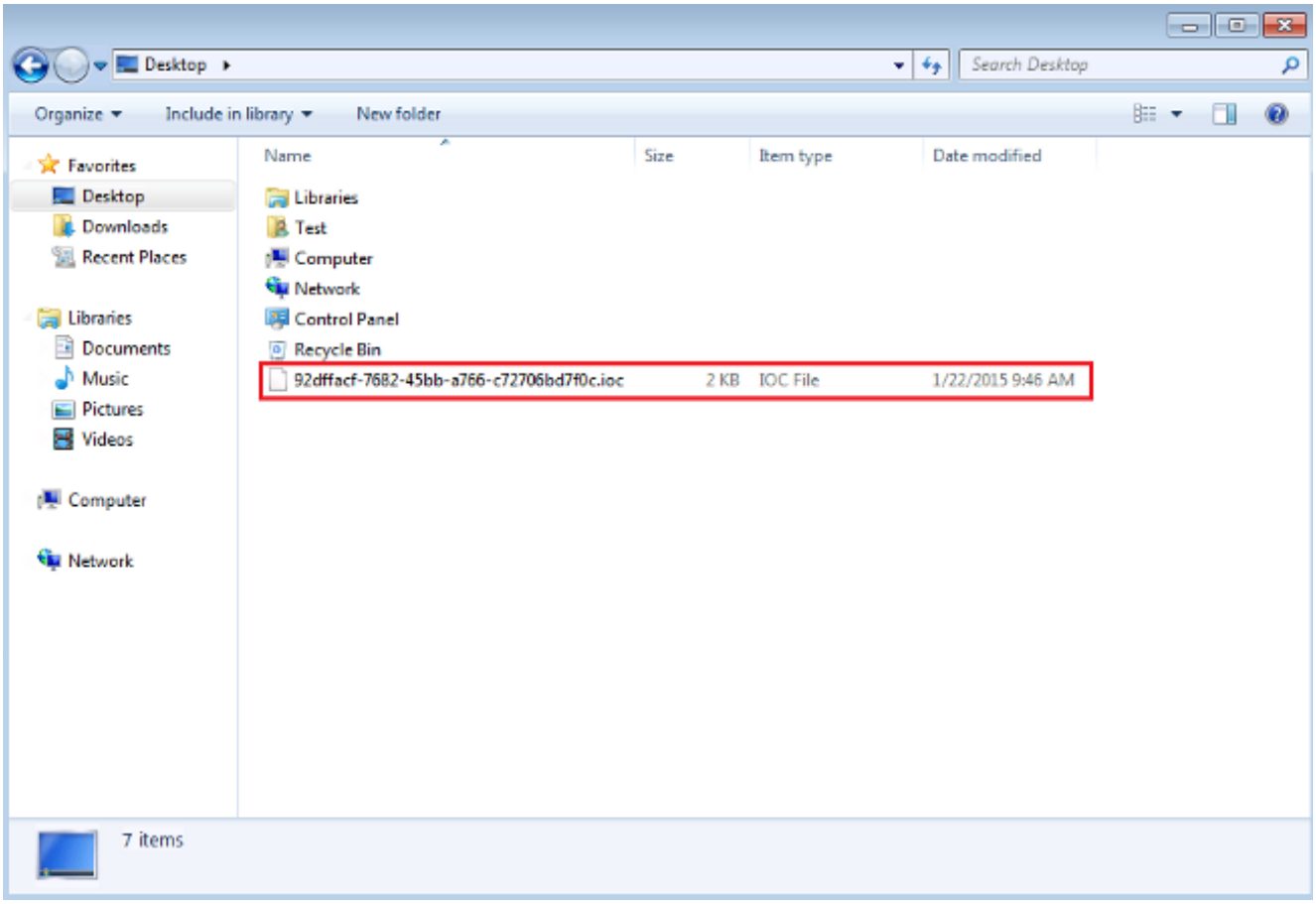
3. Nachdem Sie eine Eigenschaft hinzugefügt haben, klicken Sie auf das kleine Symbol ganz rechts im Bildschirm, um den Konfigurationsbereich zu öffnen. Verwenden Sie in diesem Bereich das Feld **Inhalt**, um eine Dateierweiterung zuzuordnen. Fügen Sie z. B. **txt hinzu**, um der **test.txt**-Textdatei zu entsprechen:



4. Sie müssen jetzt einen logischen Operator hinzufügen. In diesem Beispiel stimmen Sie der **Testtextdatei** zu. Verwenden Sie einen *AND*-Operator, und fügen Sie die nächste Eigenschaft hinzu, um diese abzugleichen. Suchen Sie den Dateinamen, und wählen Sie ihn im Strukturmenü **Artikel aus**. Fügen Sie im Bereich Eigenschaften den Namen der Datei hinzu, die Sie suchen möchten. Fügen Sie z. B. **test** im Feld Inhalt hinzu:



5. Da für diesen einfachen IOC keine zusätzlichen Eigenschaften erforderlich sind, können Sie die Datei jetzt speichern. Klicken Sie auf **Datei > Speichern**, und eine Signaturdatei mit der Erweiterung **.ioc** wird auf dem System gespeichert:



IOC-Signaturdatei hochladen

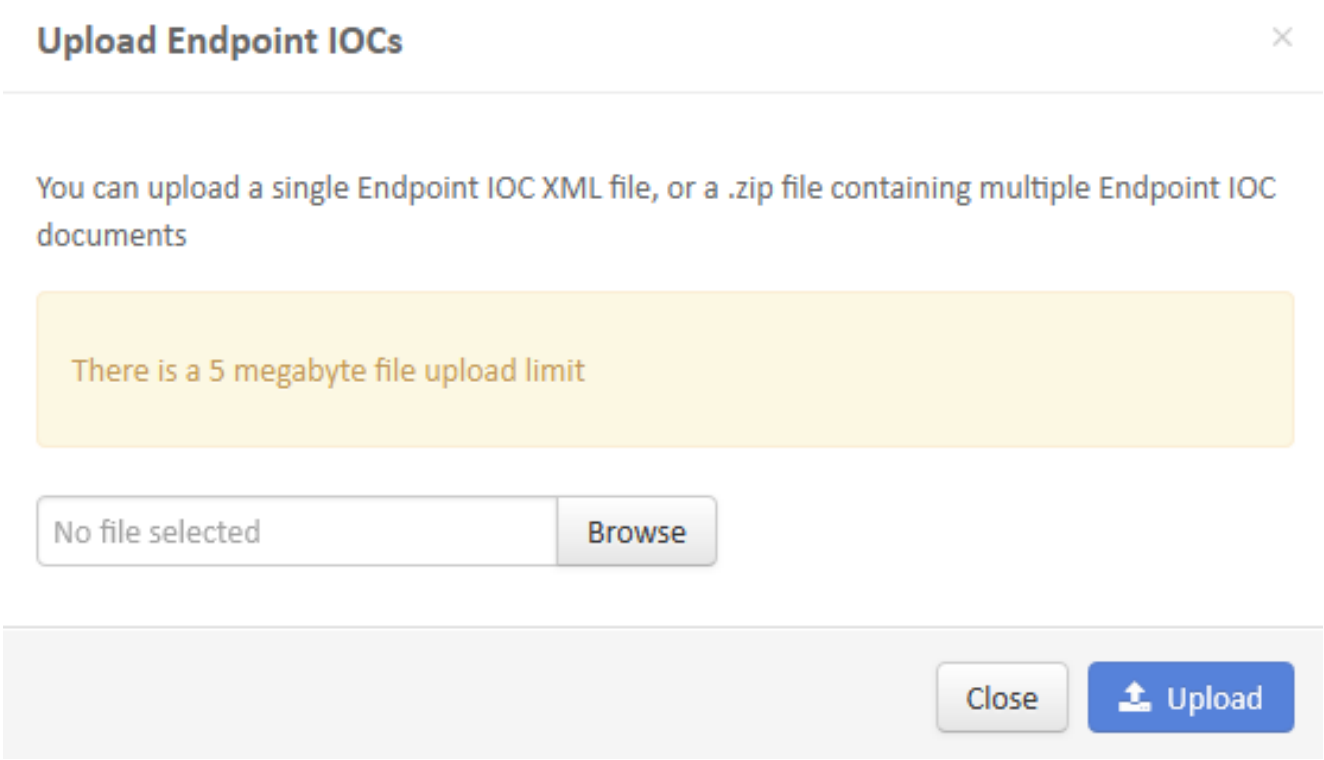
Um eine Prüfung durchzuführen, müssen Sie eine IOC-Datei auf das FireAMP-Dashboard hochladen. Sie können eine IOC-Signaturdatei, eine XML-Datei oder ein Zip-Archiv verwenden, das mehrere IOC-Dateien enthält. Das Dashboard dekomprimiert und analysiert die Datei mit den IOC-Signaturen. Sie werden benachrichtigt, wenn eine falsche Syntax oder eine nicht unterstützte Eigenschaft verwendet wird.

Tipp: Sie können Dateien mit einer Größe von bis zu fünf Megabyte hochladen.

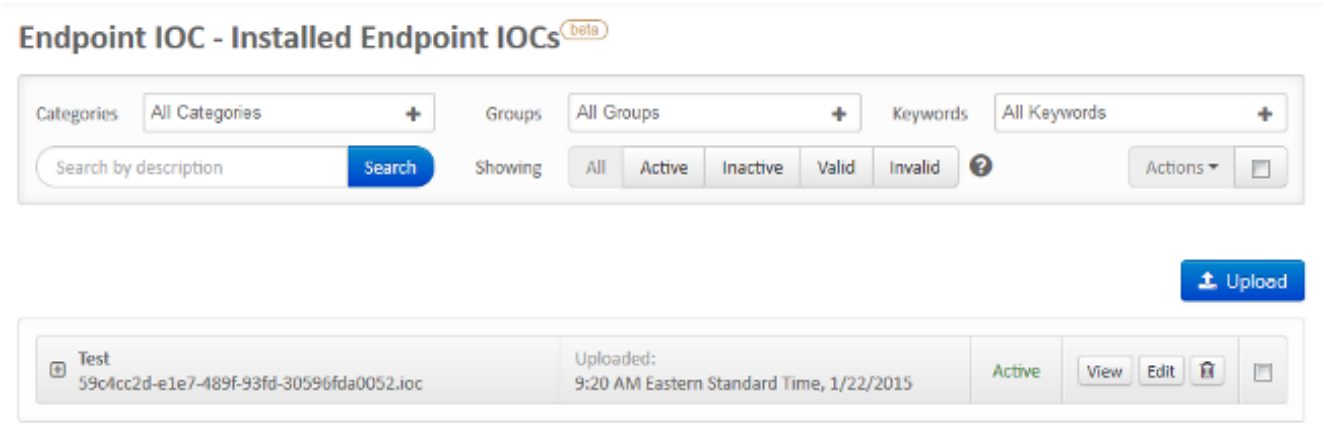
Gehen Sie wie folgt vor, um die IOC-Signaturdatei in das FireAMP-Dashboard hochzuladen:

1. Melden Sie sich bei der FireAMP Cloud Console an, und navigieren Sie zu **Outbreak Control > Installed Endpoint IOC**.

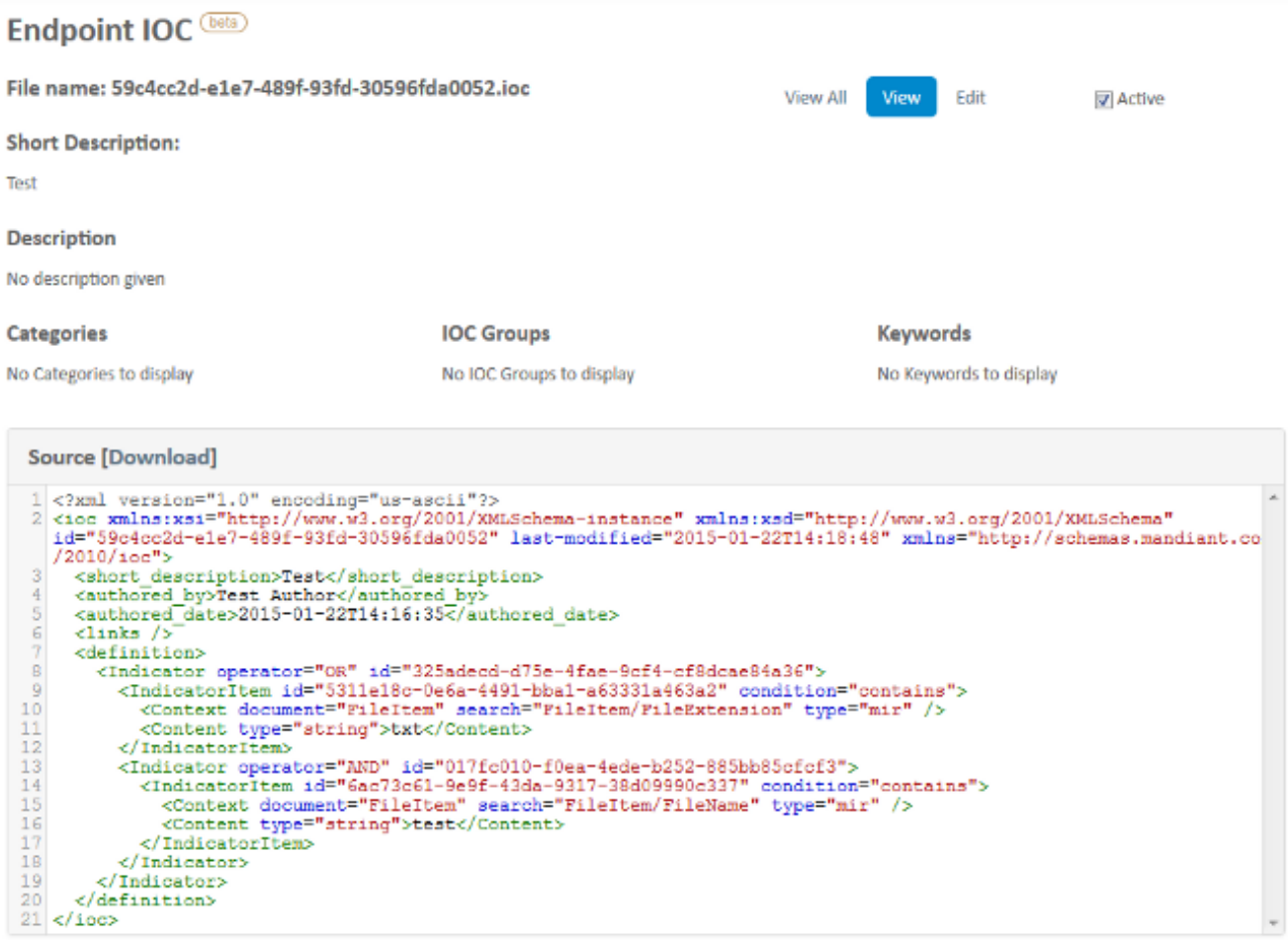
2. Klicken Sie auf **Hochladen**, und das Fenster **IOCs hochladen** wird angezeigt:



Nachdem eine IOC-Signaturdatei erfolgreich hochgeladen wurde, wird die Signatur in der Liste angezeigt:



3. Klicken Sie auf **Anzeigen**, um die tatsächlichen XML-Daten der Signatur anzuzeigen:



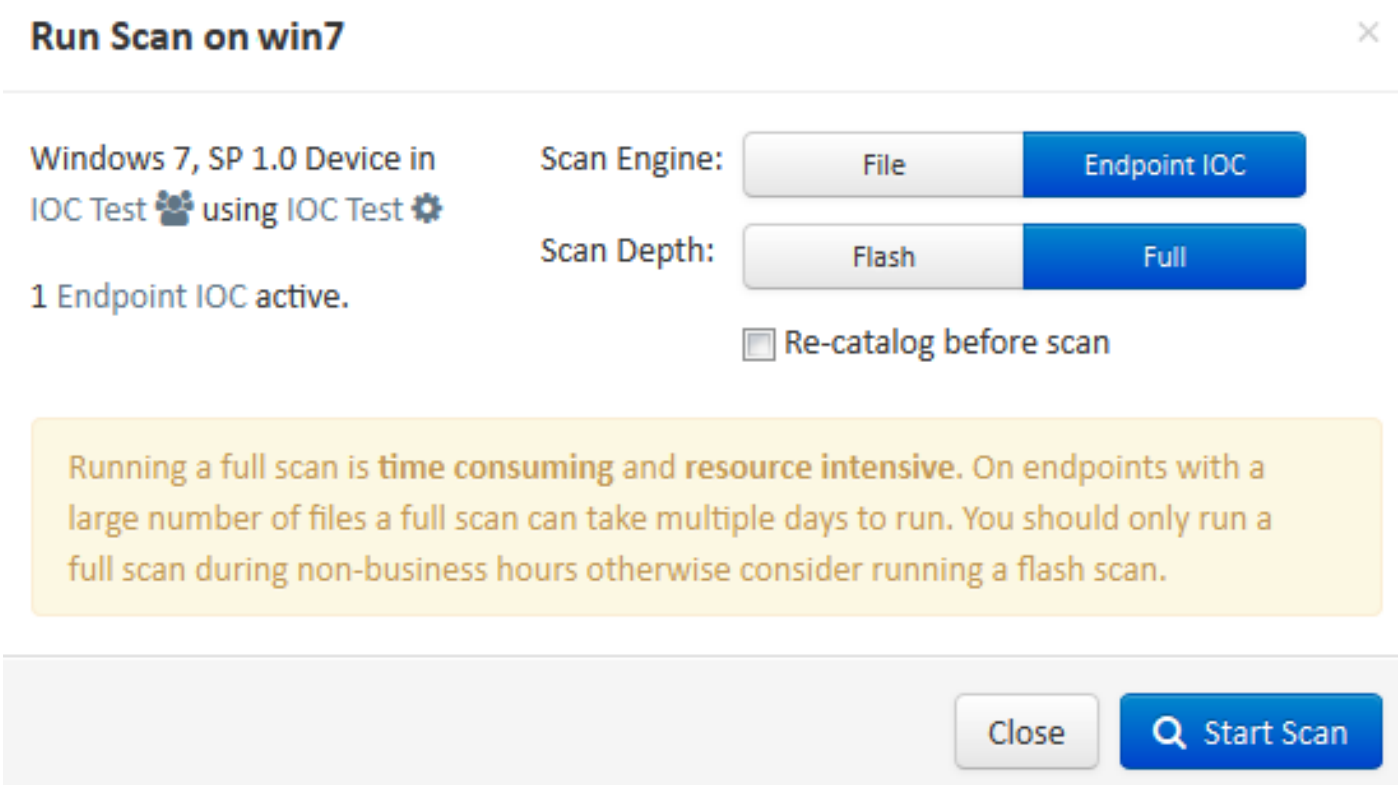
Scannen starten

Nachdem Sie eine Signaturdatei hochgeladen haben, führen Sie eine *vollständige* Prüfung durch. Bei der ersten Prüfung muss es sich um eine vollständige Prüfung handeln, da ein Metadatenkatalog für den gesamten Computer erstellt werden muss, der 1-2 Stunden dauern kann. Sie können eine *Flash*-Prüfung durchführen, nachdem das System durch eine vollständige Systemprüfung katalogisiert wurde.

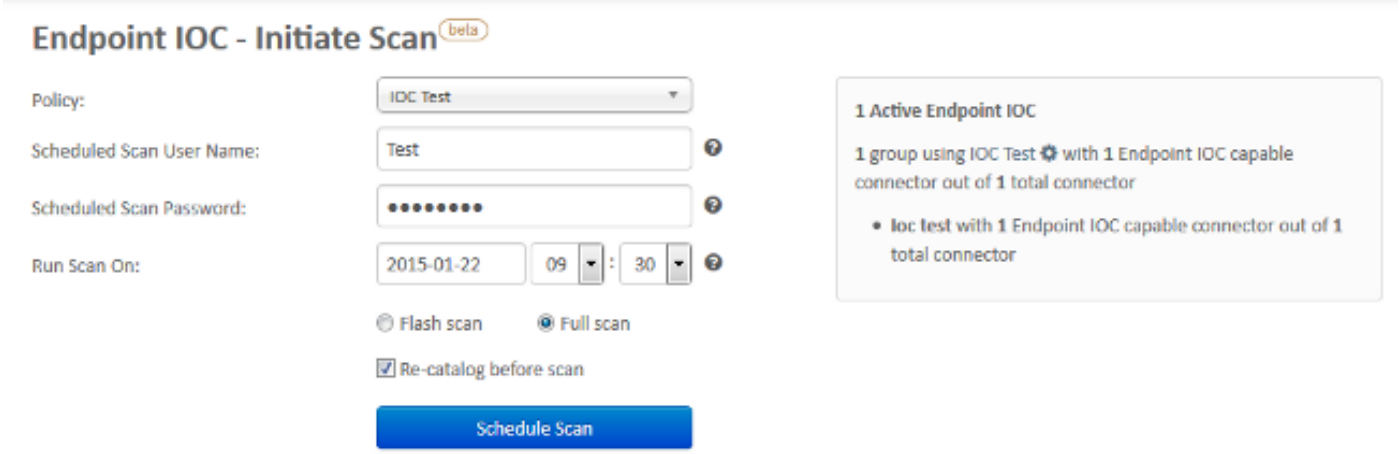
> **Hinweis**: Der vollständige Scan ist sehr CPU-intensiv. Cisco empfiehlt, während der Verwendung keine vollständige Systemprüfung auf einem Computer durchzuführen. Wenn Sie planen, die Funktion regelmäßig zu verwenden, können Sie einmal im Monat eine vollständige Prüfung durchführen, um den Katalog neu zu erstellen.

Sie können zwei verschiedene Methoden verwenden, um eine IOC-Prüfung auszuführen. Die erste Methode besteht darin, eine sofortige Prüfung von einem Ereignis oder vom Dashboard aus durchzuführen. Dies wird beim nächsten Senden eines Heartbeat an die Cloud durch einen PC ausgelöst.

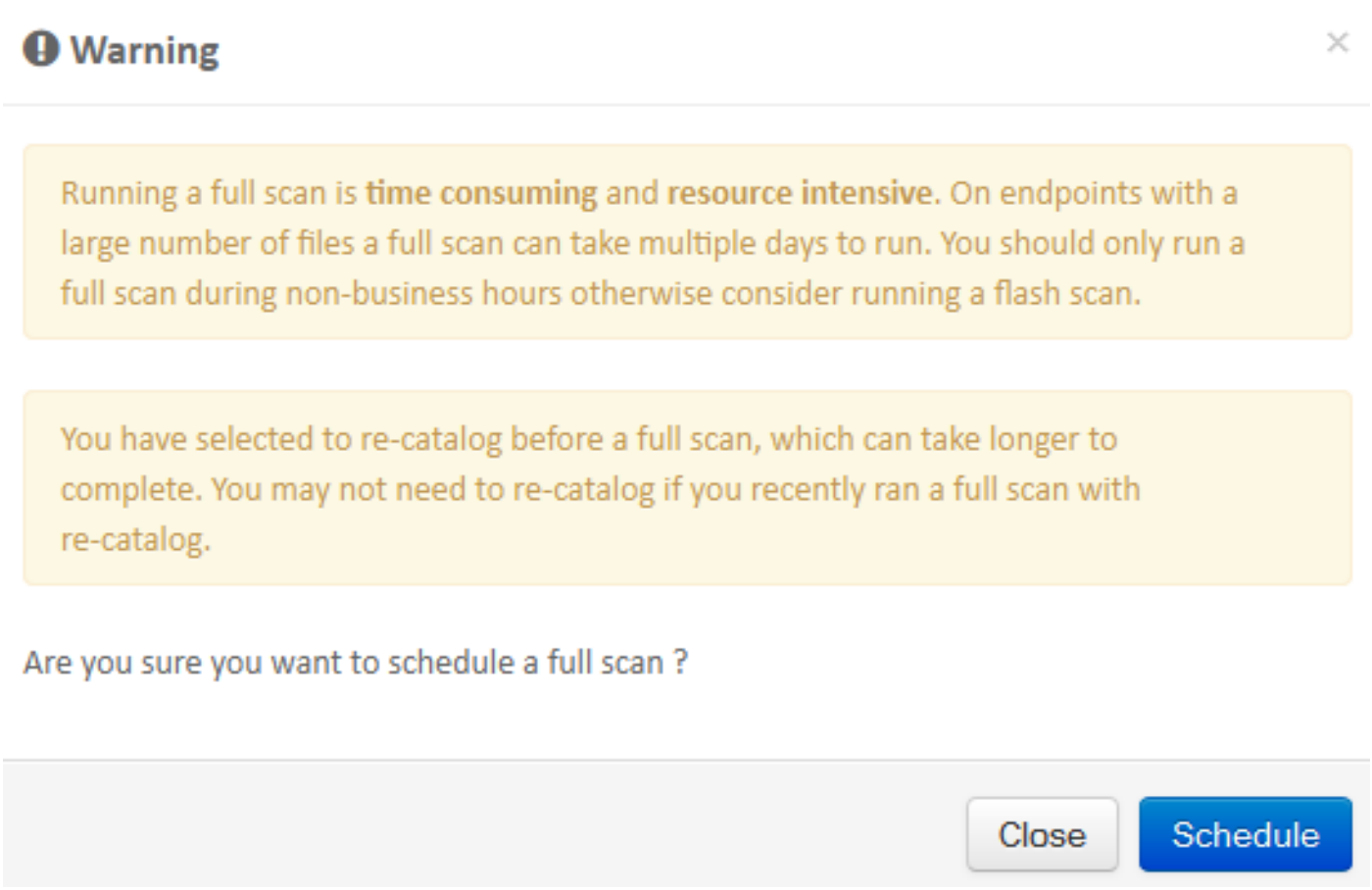
> **Hinweis**: Wenn Sie die vollständige Prüfung zum ersten Mal durchführen, müssen Sie die Option **Re-catalog** nicht **vor dem Scannen** überprüfen.



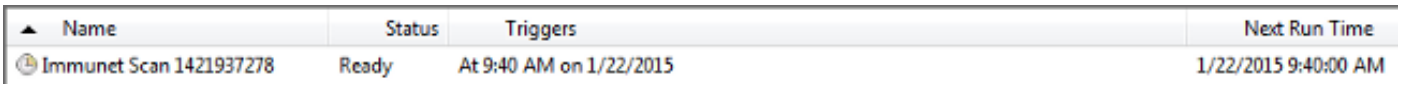
Die zweite Methode besteht darin, eine geplante IOC-Prüfung für Endpunkte im Menü **Outbreak-Kontrolle** des Dashboards zu erstellen. Diese Option ist möglicherweise ideal, wenn außerhalb der Spitzenzeiten Prüfungen durchgeführt werden sollen. Sie müssen die Anmeldeinformationen eines Kontos angeben, das über Berechtigungen für den angegebenen Computer verfügt, um geplante Aufgaben zu erstellen und die Berechtigung **Als Stapelgruppenrichtlinie anmelden** zuzulassen.



Wenn Sie eine Endpunkt-IOC-Prüfung planen, wird folgende Warnmeldung angezeigt:

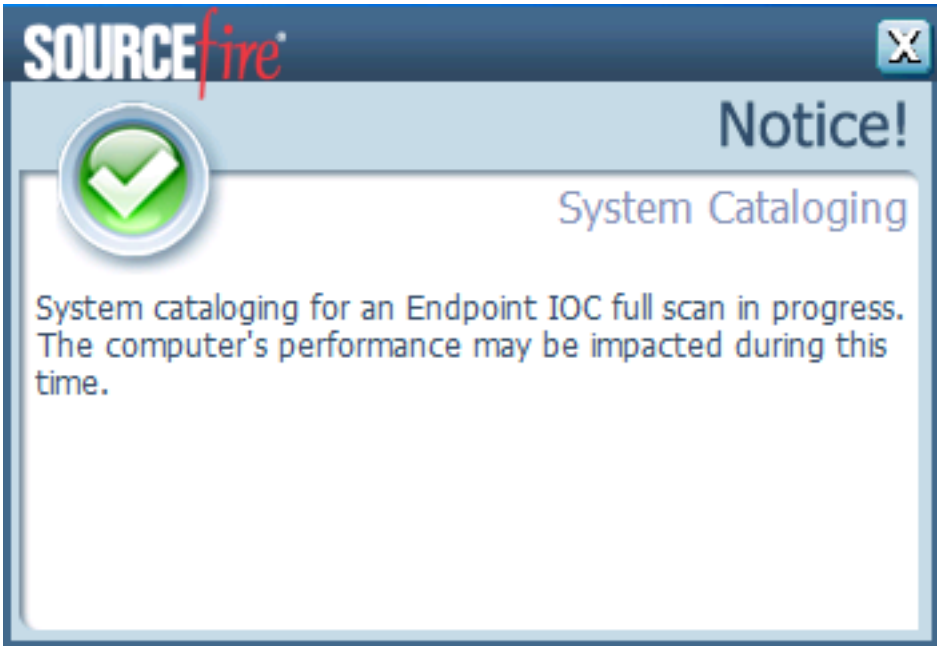


Wenn Ihr Computer das nächste Mal einen Heartbeat sendet und Ihre Anmeldeinformationen gültig sind, sollten Sie einen Job ähnlich dem in der Windows-Aufgabenplanung sehen:



Wenn die Prüfung gestartet wird, wird folgende Meldung angezeigt:

> **Hinweis**: Wenn die GUI so konfiguriert ist, dass sie ausgeblendet wird, wird der Hinweis zur **Systemkatalogierung** nicht angezeigt.



Wenn die Prüfung abgeschlossen ist, können Sie die *Zusammenfassung der Endpunkt-IOC-Scan-Erkennung* anzeigen. Dieses Beispiel zeigt eine Übereinstimmung für die **test.txt-**IOC-Signaturdatei: