Endpoint IOC-scans uitvoeren met AMP voor endpoints of FirePOWER

Inhoud

Inleiding

Dit document beschrijft hoe u een bestand voor de ondertekening van een compromis (IOC) kunt maken via de Mandiant IOC-editor, hoe u het kunt uploaden naar het Cisco FireAMP-dashboard en hoe u een IOC-scan van een eindpunt kunt openen.

Voorwaarden

Vereisten

Cisco raadt u aan ten minste één gigabyte vrije ruimte in te stellen voordat u probeert de eindpunten IOC-scans te gebruiken.

Gebruikte componenten

De informatie in dit document is gebaseerd op de scanner voor endpoints OC, die beschikbaar is in de versies 4.0.2 en hoger van Cisco FirePOWER Windows Connector.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

De functie voor het instellen van een IOC-scanner is een krachtig instrument voor respons op incidenten, dat wordt gebruikt om post-compromisindicatoren op meerdere computers te scannen.

> **Opmerking:** Hoewel FireAMP IOCs met de Mandiant-taal ondersteunt, wordt de Mandiant IOC Editor-software zelf niet ontwikkeld of ondersteund door Cisco. Cisco-ondersteuning geeft geen problemen met de door de gebruiker gemaakte of door derden gemaakte OC's.

IOS-signaalbestanden

Het IOC-bestand voor handtekeningen is een verlengbaar XML-schema voor de beschrijving van technische kenmerken die een bekende bedreiging, een aanslagmethodologie of ander compromisbewijs identificeren.

U kunt endpoints IOC's door de console importeren uit op OpenIOC gebaseerde bestanden die zijn geschreven om bestandseigenschappen zoals naam, grootte en hash, evenals andere eigenschappen en systeemeigenschappen zoals procesinformatie, actieve services en Microsoft Windows Registeritems te activeren. De syntaxis van de IOC kan worden gebruikt door de respons van het incident om specifieke artefacten te vinden of om de logica te gebruiken om complexe, gecorreleerde detecties te creëren voor families van malware.

Start een scan van een IOC-bestand

Er zijn drie stappen die u moet uitvoeren om een scan in een IOC-bestand met handtekeningen te kunnen uitvoeren:

1. Maak een OCR-bestand.
2. Upload het IOC-bestand voor handtekeningen.
3. Start een scan.

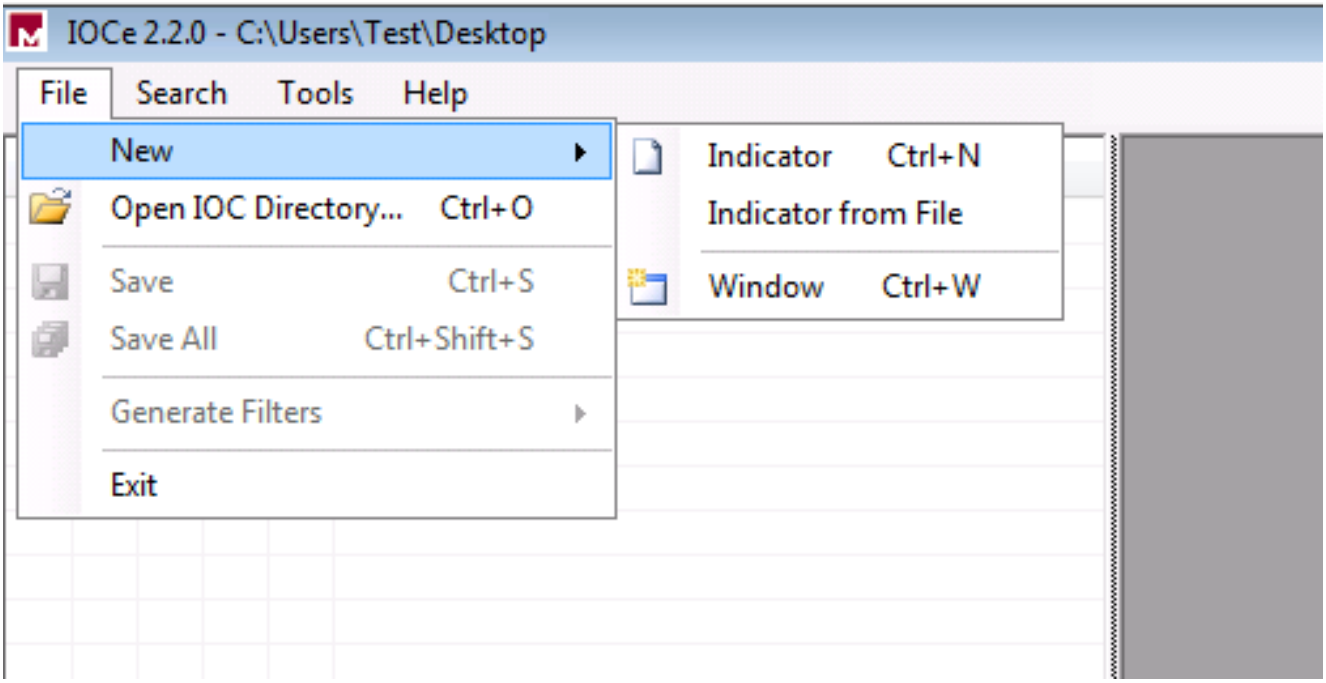
Deze stappen worden uitgebreid in de volgende secties.

Een IOC-signaalbestand maken

> **Opmerking:** In dit voorbeeld, wordt de Mandiant IOC redacteur gebruikt om een IOC signatebestand te bouwen voor een tekstbestand genaamd **test.txt**.

Voltooi deze stappen om een IOC-bestand voor handtekeningen te maken:

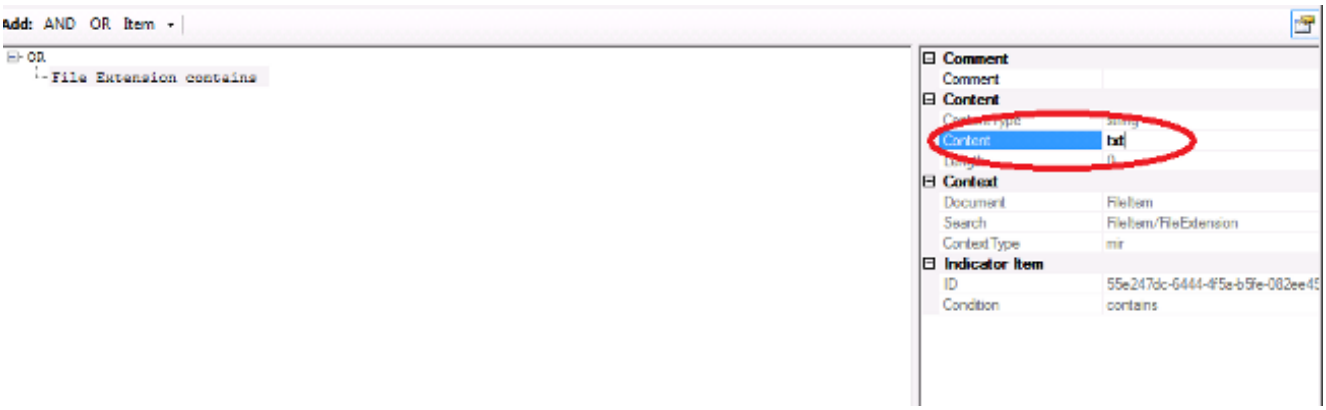
1. Open de **IOCe** en navigeer naar **Bestand > Nieuw > Indicator**. Dit biedt een lege werkruimte zodat u kunt beginnen met het bouwen van een IOC.



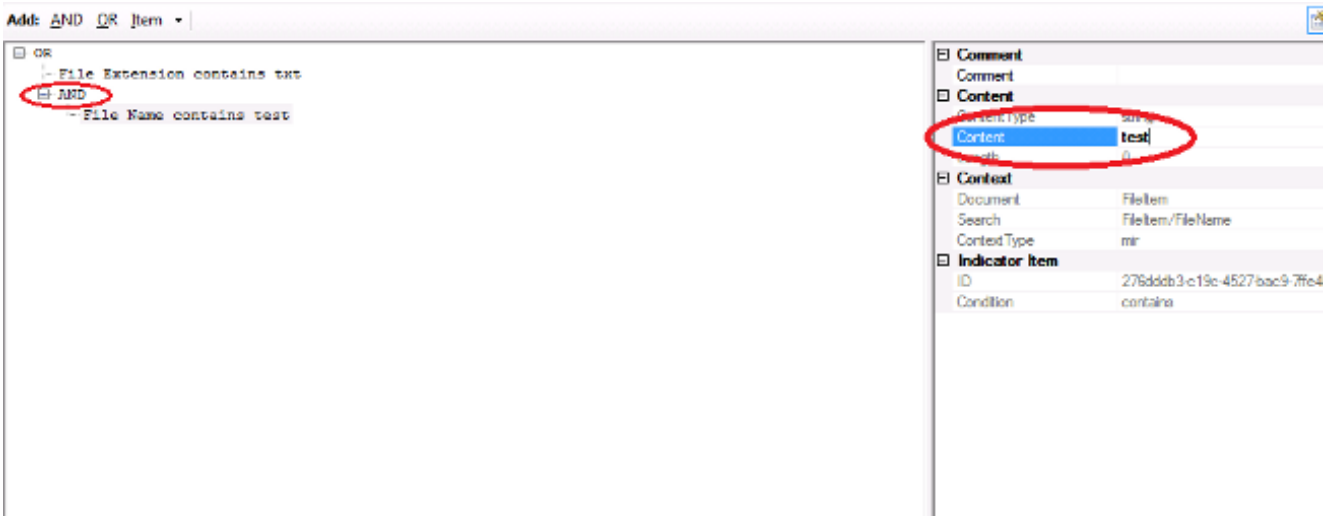
Opmerking: Om een IOC voor iets specifieks te maken, gebruik binaire logica met de eigenschappen. De eerste exploitant is een OR, de eenvoudigste basis om van te werken. Hierdoor kan de initiële functie van de IOC werken, dus je hoeft deze niet te wijzigen. Het is vereist dat een IOC-bestand voor handtekening ten minste twee eigenschappen of voorwaarden heeft om het in een scan succesvol te kunnen gebruiken.

2. Klik op het vervolgkeuzemenu Opties om operatoren toe te voegen. De eerste eigenschap die u moet toevoegen is **File Extension bevat**. Vind de eigenschap in het menu **Items** en klik op deze.

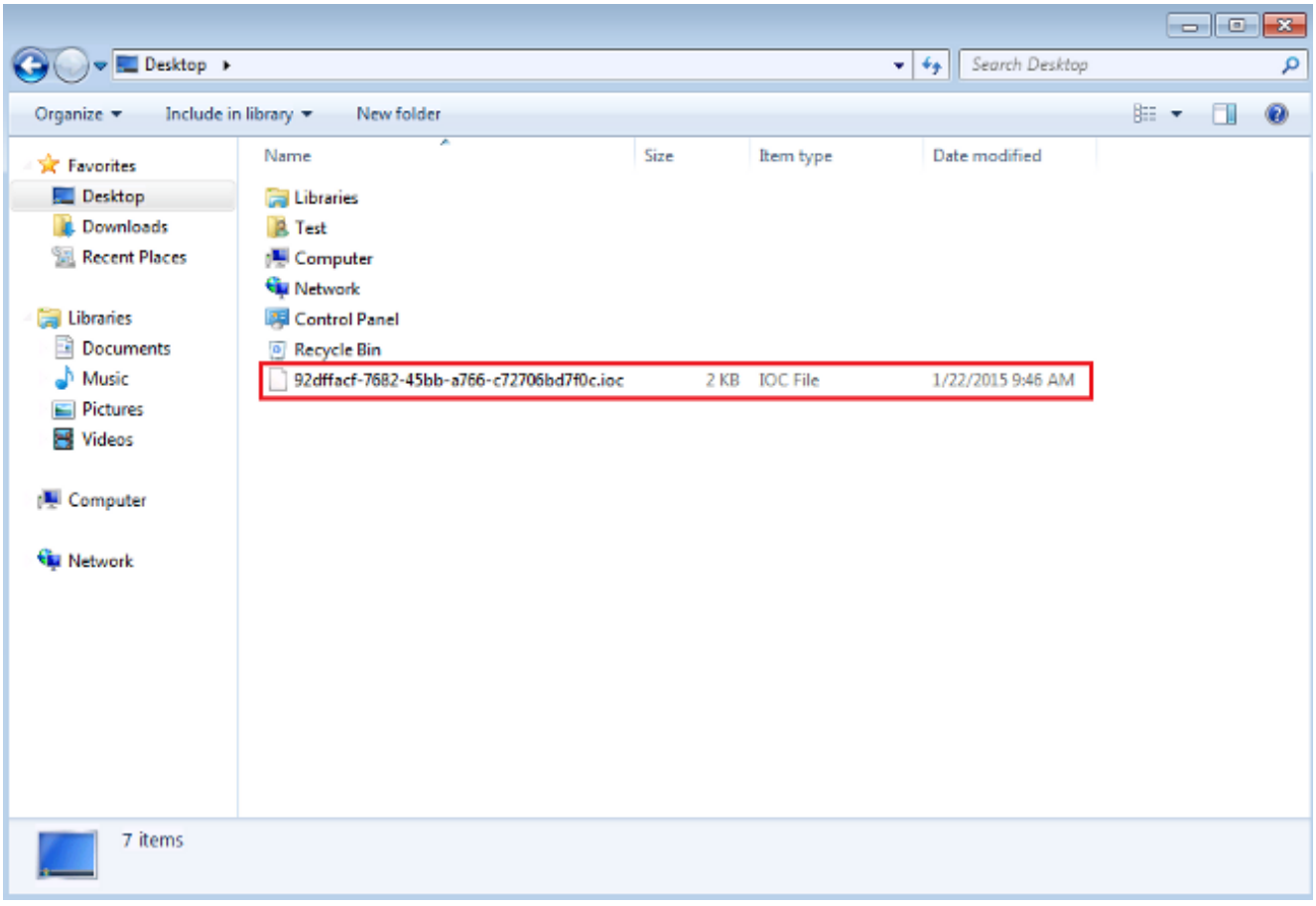
3. Nadat u een eigenschap hebt toegevoegd, klikt u op het kleine pictogram aan de rechterkant van het scherm om het Configuratiescherm te openen. Gebruik in dit venster het veld **Content** om een bestandsextensie overeen te komen. Voeg bijvoorbeeld **tekst toe** om het tekstbestand **test.txt** aan te passen:



4. U moet nu een logische operator toevoegen. In dit voorbeeld komt u overeen met het **testtekstbestand**. Om dit aan te passen, gebruik een *EN* exploitant en voeg het volgende bezit toe. Zoek de bestandsnaam en selecteer deze in het menu **Items**. Voeg in het venster Eigenschappen de naam toe van het bestand dat u wilt vinden. Voeg bijvoorbeeld **test toe** in het veld Inhoud:



5. Aangezien voor deze eenvoudige IOC geen extra eigenschappen nodig zijn, kunt u het bestand nu opslaan. Klik op **Bestand > Opslaan** en een bestand met een **.ioc-**extensie wordt op het systeem opgeslagen:



Een OCR-bestand uploaden

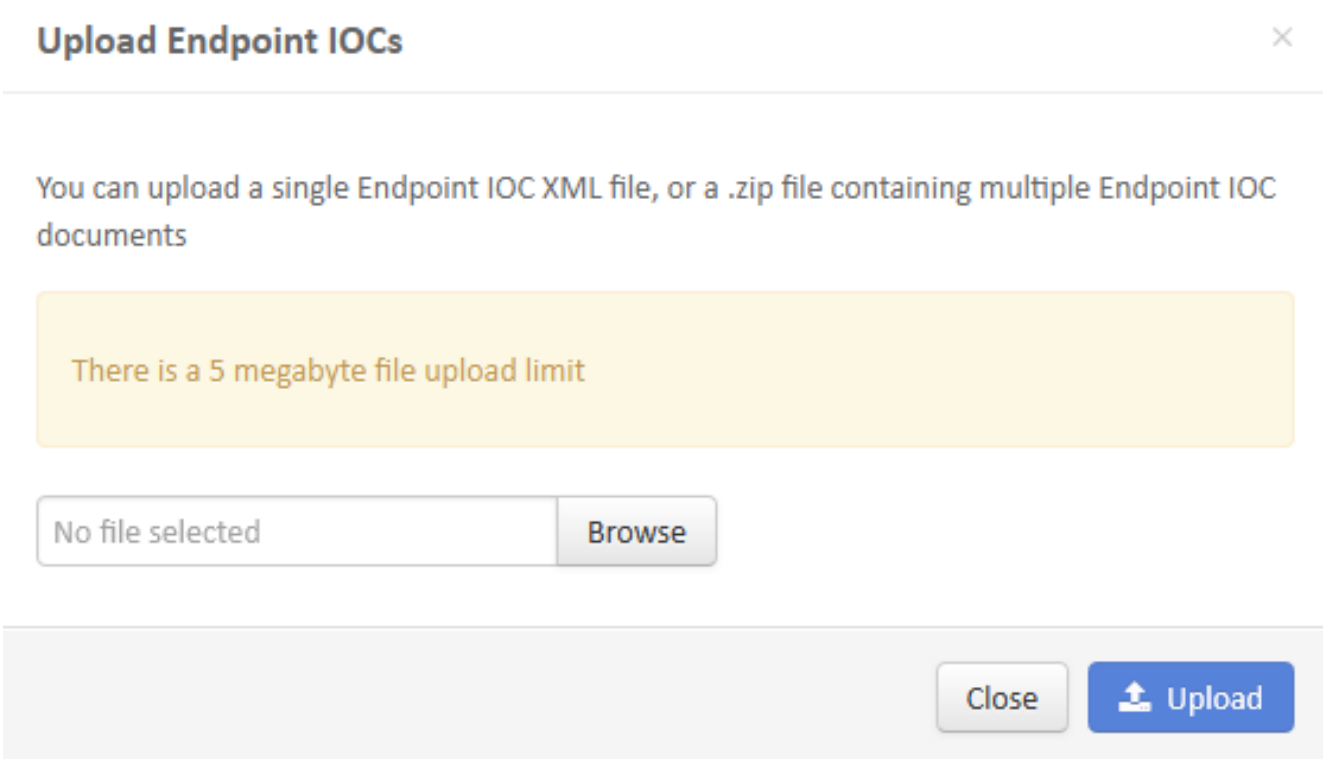
Om een scan te kunnen uitvoeren, moet u een IOC-bestand naar het FireAMP-dashboard uploaden. U kunt een IOC-bestand, een XML-bestand of een zip-archief gebruiken dat meerdere IOC-bestanden bevat. Het dashboard wordt gedecomprimeerd en geparkeerd, terwijl de IOC-handtekeningen worden gebruikt. U wordt op de hoogte gesteld als een onjuiste syntax of een niet-ondersteunde eigenschap wordt gebruikt.

Tip: U kunt bestanden van maximaal vijf megabytes in grootte uploaden.

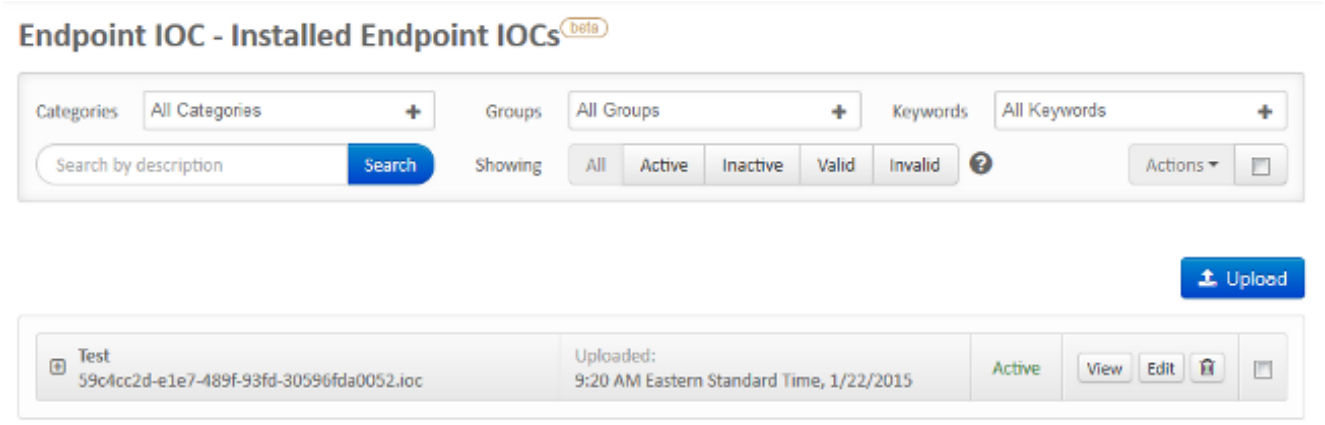
Voltooi deze stappen om het OCR-bestand met handtekeningen naar het FireAMP-dashboard te uploaden:

1. Meld u aan bij de FireAMP Cloud-console en navigeer naar **Outdoorkleding Control > Geïnstalleerd endpoint IOC**.

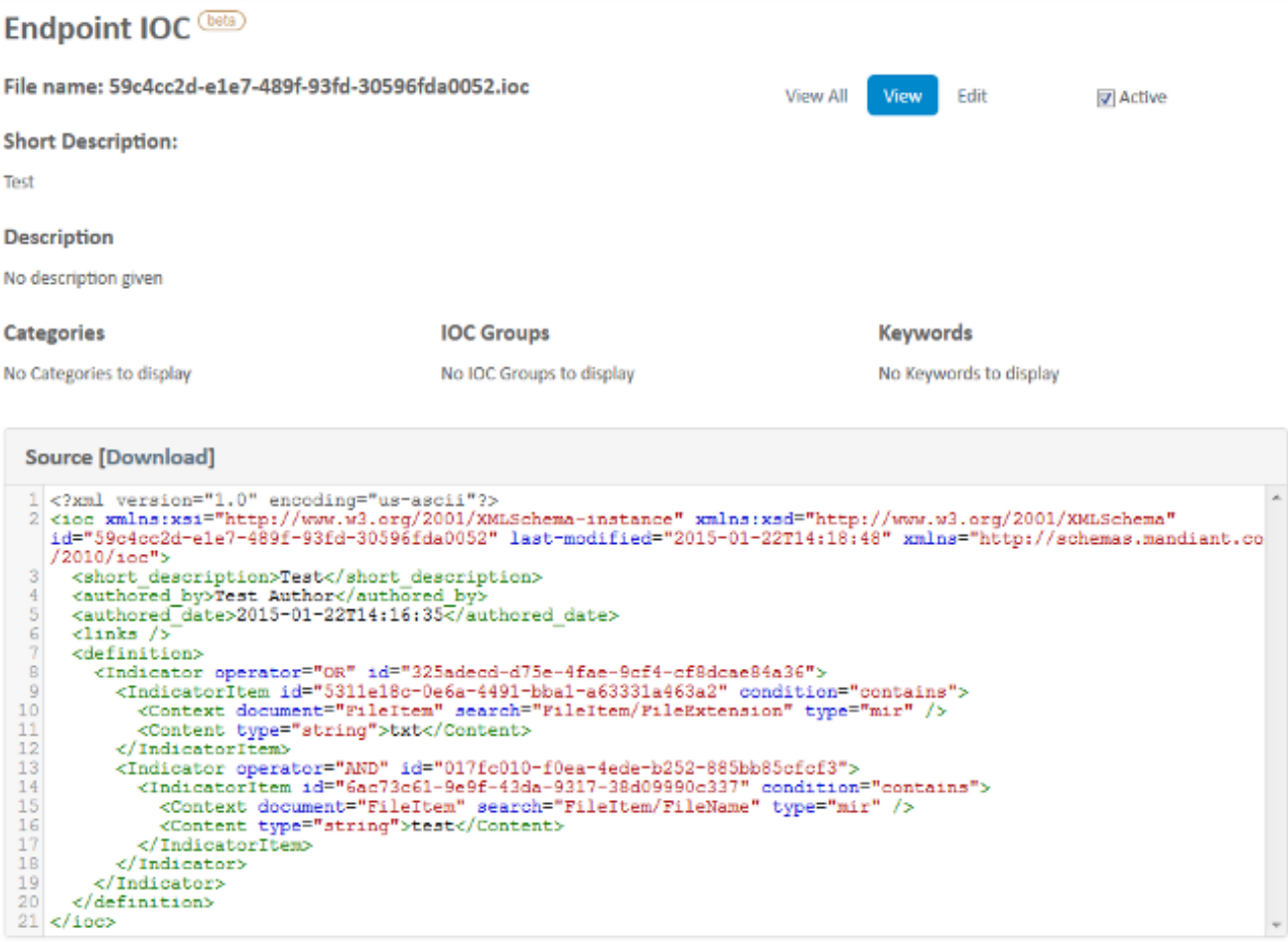
2. Klik op **Upload** en het venster **Upload Endpoint IOCs** verschijnt:



Nadat een OCR-bestand met handtekeningen is geüpload, verschijnt de handtekening in de lijst:



3. Klik op **View** om de eigenlijke XML gegevens van de handtekening te bekijken:



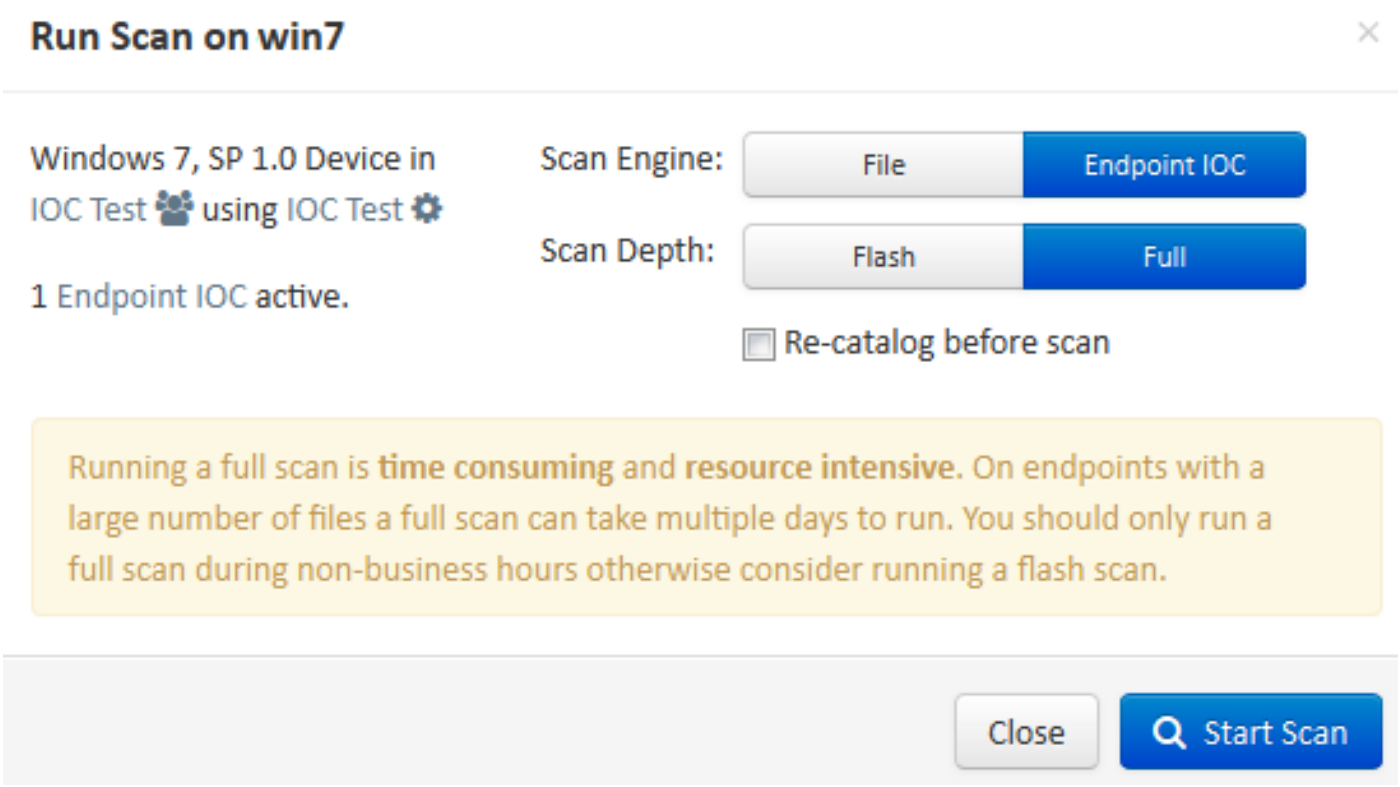
Een scan openen

Nadat u een bestand met handtekeningen hebt geüpload, voert u een *volledige* scan uit. De eerste scan moet een volledige scan zijn, omdat het een catalogus met metagegevens voor de gehele computer moet maken, die 1-2 uur kan duren. U kunt een flitsscan uitvoeren nadat het systeem is gecatalogiseerd via een volledige scan.

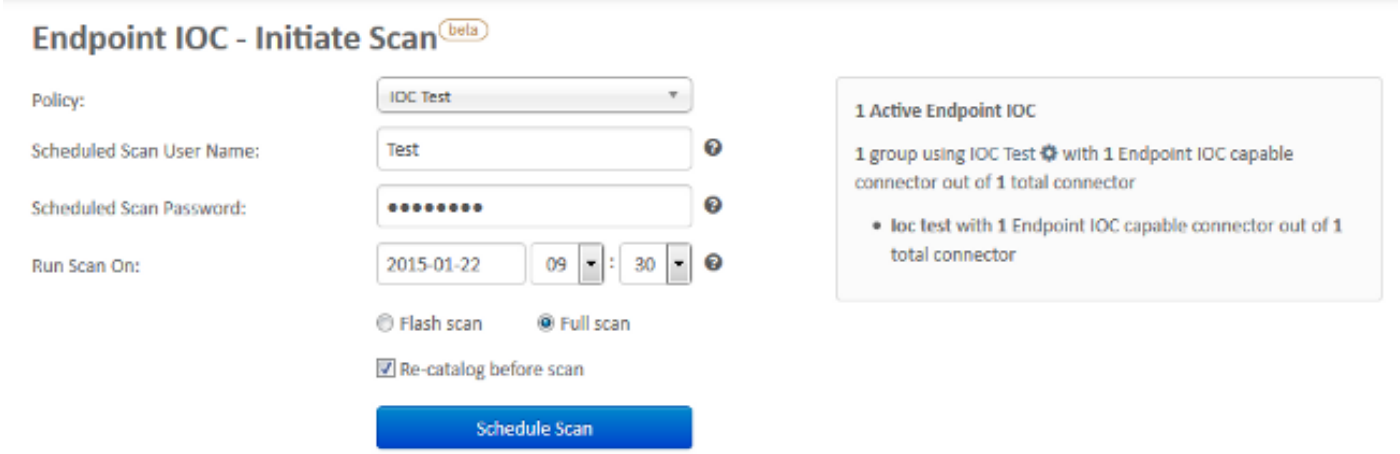
> **Opmerking:** De volledige scan is zeer CPU-intensief. Cisco raadt u aan geen volledige scan op een pc te maken terwijl het apparaat in gebruik is. Als u de functie regelmatig wilt gebruiken, kunt u een volledige scan per maand uitvoeren om de catalogus te herbouwen.

Er zijn twee verschillende methoden die u kunt gebruiken om een IOC-scan te maken. De eerste methode is om een directe scan van een gebeurtenis of van het dashboard uit te voeren. Dit wordt de volgende keer geactiveerd dat een PC een hartslag naar de Cloud stuurt.

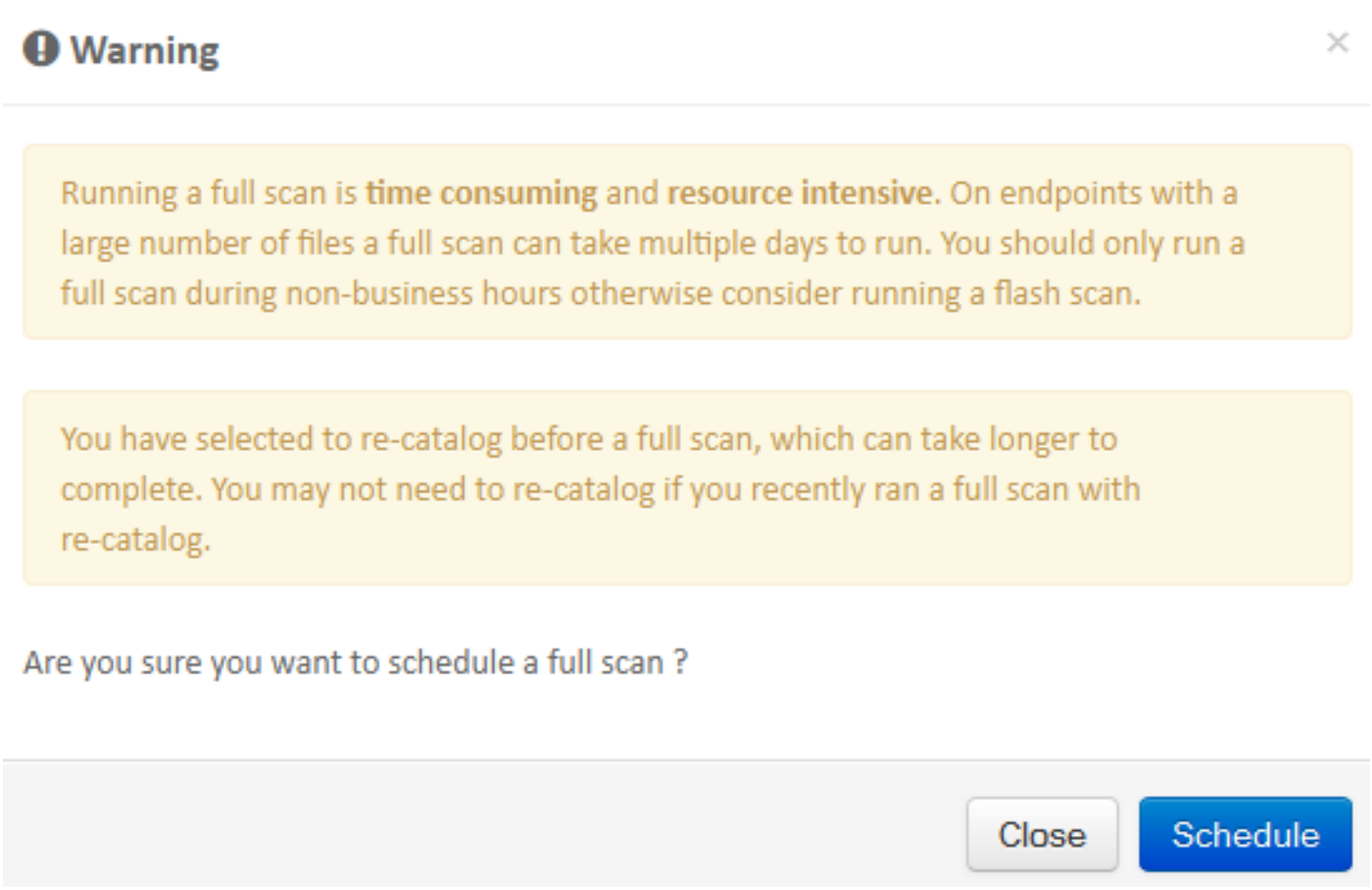
> **Opmerking:** Als dit de eerste keer is dat u de volledige scan uitvoert, hoeft u de **hercatalogus** niet **opnieuw te** controleren **voordat u** de optie **scant**.



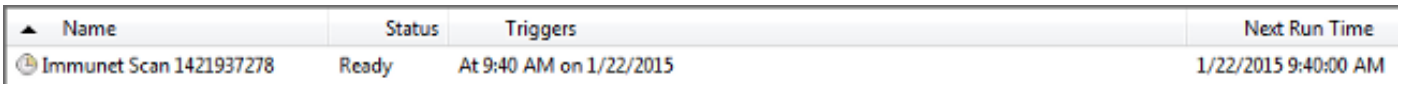
De tweede methode is om een geplande IOC-scan van het **Outbreak Control-**menu van het dashboard te maken. Deze optie kan ideaal zijn wanneer u scans tijdens uren buiten de piek wilt uitvoeren. U moet de aanmeldingsgegevens van een account met toestemming op de gegeven computer opgeven om geplande taken te maken en het **inloggen als** toestemming voor een Batch-groepsbeleid mogelijk te maken.



Wanneer u een OC-scan van het eindpunt plant, verschijnt dit waarschuwingsbericht:

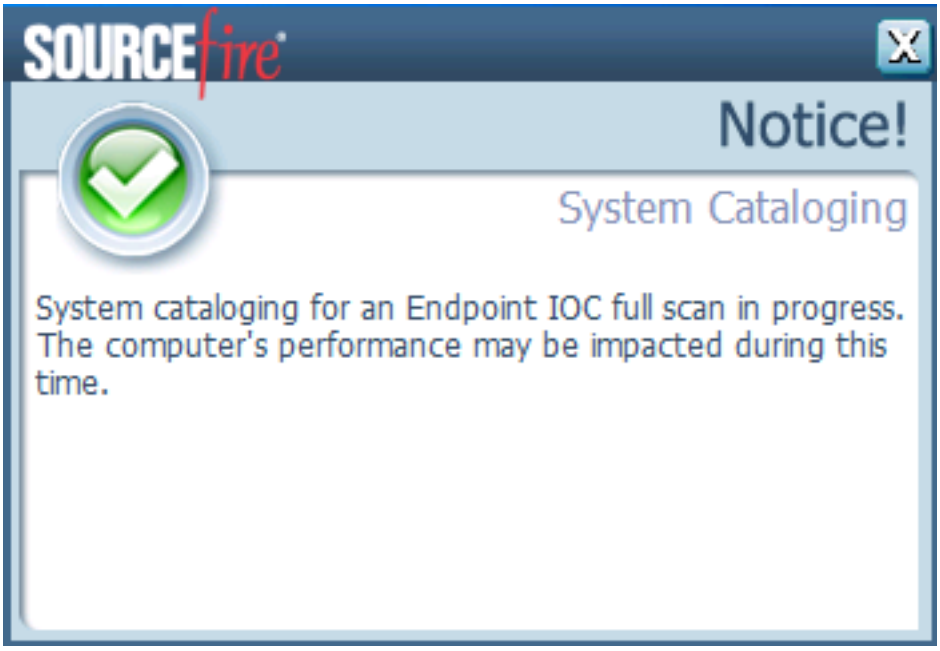


De volgende keer dat uw PC een hartslag verstuurt en als uw geloofsbrieven geldig zijn, zou u een baan moeten zien die aan dit in de taakplanner van Windows lijkt:



Wanneer de scan begint, verschijnt dit bericht:

> **Opmerking:** Als de GUI ingesteld is om verborgen te zijn, dan ziet u het bericht **Systeemcatalogiseren** niet.



Wanneer de scan is voltooid, kunt u de *samenvatting van* de *endpointdetectie IOS* van *scan* bekijken. Dit voorbeeld toont een match voor het bestand van de handtekening van **test.txt** IOC: