AMP for Endpoints 또는 FireAMP로 엔드포인트 IOC 스캔 수행

목차

소개

이 문서에서는 Mandiant IOC 편집기를 통해 IOC(Indication of Compromise) 시그니처 파일을 생성하는 방법, 이를 Cisco FireAMP 대시보드에 업로드하는 방법 및 엔드포인트 IOC 스캔을 시작하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

엔드포인트 IOC 스캔을 실행하기 전에 1GB 이상의 사용 가능한 드라이브 공간이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco FireAMP Windows Connector 버전 4.0.2 이상에서 제공되는 엔드포인트 IOC 스캐너를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

엔드포인트 IOC 스캐너 기능은 여러 컴퓨터에서 감염 후 지표를 스캔하는 데 사용되는 강력한 사고 대응 툴입니다.

> **참고:** FireAMP는 Mandiant 언어로 IOC를 지원하지만 Mandiant IOC Editor 소프트웨어 자체는 Cisco에서 개발하거나 지원하지 않습니다. Cisco 지원에서는 사용자가 생성한 IOC 또는 서드파티 IOC는 트러블슈팅하지 않습니다.

IOC 서명 파일

IOC 서명 파일은 알려진 위협, 공격자 방법론 또는 기타 보안 침해 증거를 식별하는 기술 특성에 대한 설명을 위해 확장 가능한 XML 스키마입니다.

이름, 크기, 해시와 같은 파일 속성뿐 아니라 프로세스 정보, 실행 중인 서비스, Microsoft Windows 레지스트리 항목 등의 기타 속성 및 시스템 속성을 트리거하기 위해 작성된 OpenIOC 기반 파일로부터 콘솔을 통해 엔드포인트 IOC를 가져올 수 있습니다. IOC 구문은 특정 아티팩트를 찾거나 로직을 사용하여 악성코드군에 대한 정교한 상호 연결된 탐지를 생성하기 위해 사고 대응자가 사용할 수 있습니다.

IOC 서명 파일에서 스캔 실행

IOC 서명 파일에서 스캔을 실행하려면 다음 3단계를 완료해야 합니다.

1. IOC 서명 파일을 생성합니다.
2. IOC 서명 파일을 업로드합니다.
3. 스캔을 시작합니다.

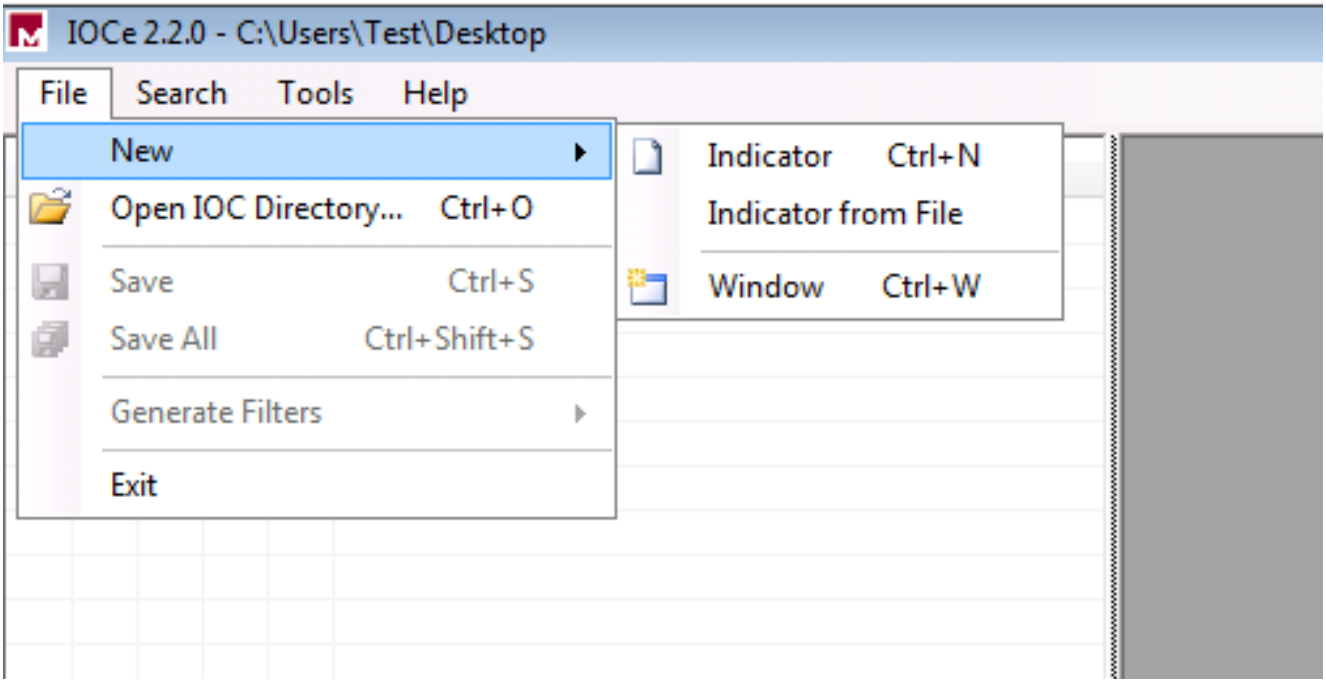
이러한 단계는 다음 섹션에서 확장됩니다.

IOC 서명 파일 생성

> **참고:** 이 예에서 Mandiant IOC 편집기는 **test.txt**라는 텍스트 파일에 대한 IOC 서명 파일을 빌드하기 위해 사용됩니다.

IOC 서명 파일을 생성하려면 다음 단계를 완료합니다.

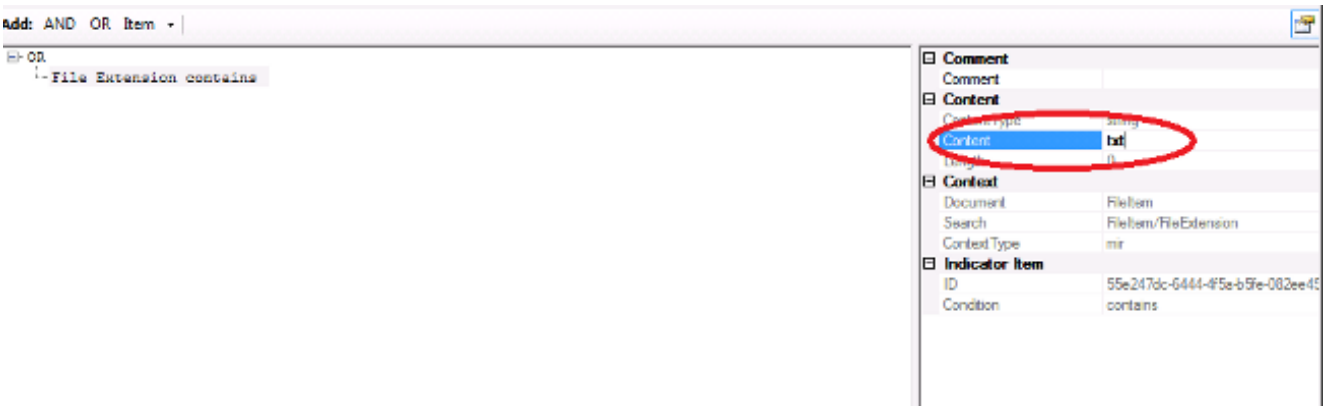
1. IOCe를 열고 **File(파일) > New(새로 만들기) > Indicator(지표)로 이동합니다**. 그러면 IOC를 구축하기 시작할 수 있는 빈 작업공간이 제공됩니다.



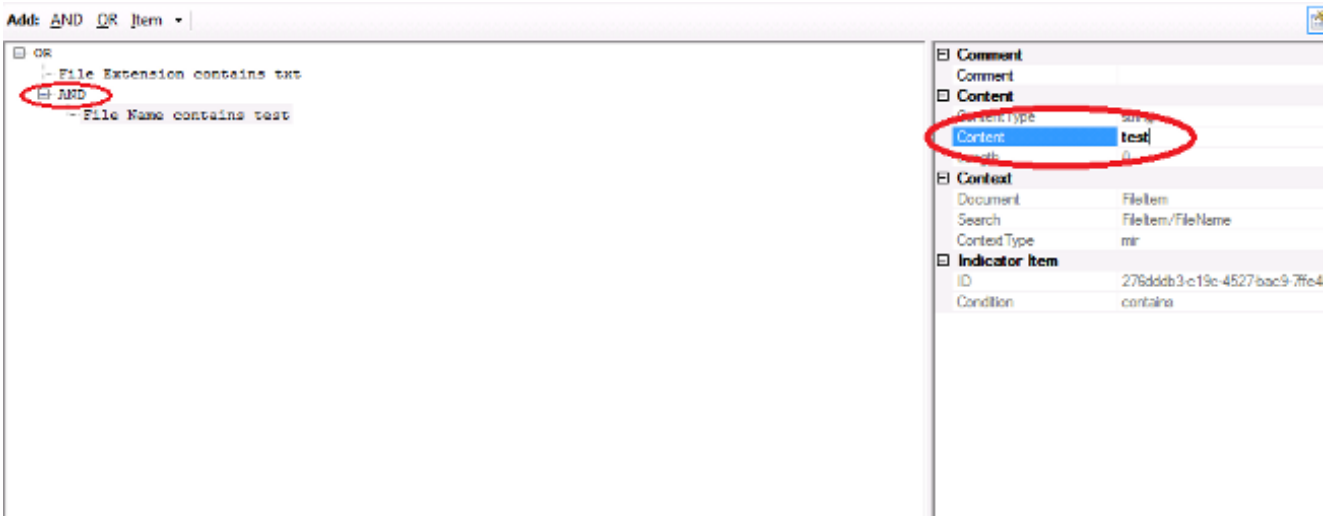
참고: 특정 항목에 대한 IOC를 생성하려면 속성에 이진 논리를 사용합니다. 초기 연산자는 OR이며, 가장 간단한 기본 작업입니다. 이렇게 하면 IOC의 초기 기능이 작동하므로 변경할 필요가 없습니다. 스캔에서 성공적으로 사용하려면 IOC 서명 파일에 적어도 두 개의 속성 또는 조건이 있어야 합니다.

2. 연산자를 추가하려면 **항목** 드롭다운 메뉴를 클릭합니다. 추가해야 하는 첫 번째 속성은 **파일 확장자**에 **포함됩니다**. **항목** 트리 메뉴에서 속성을 찾아 클릭합니다.

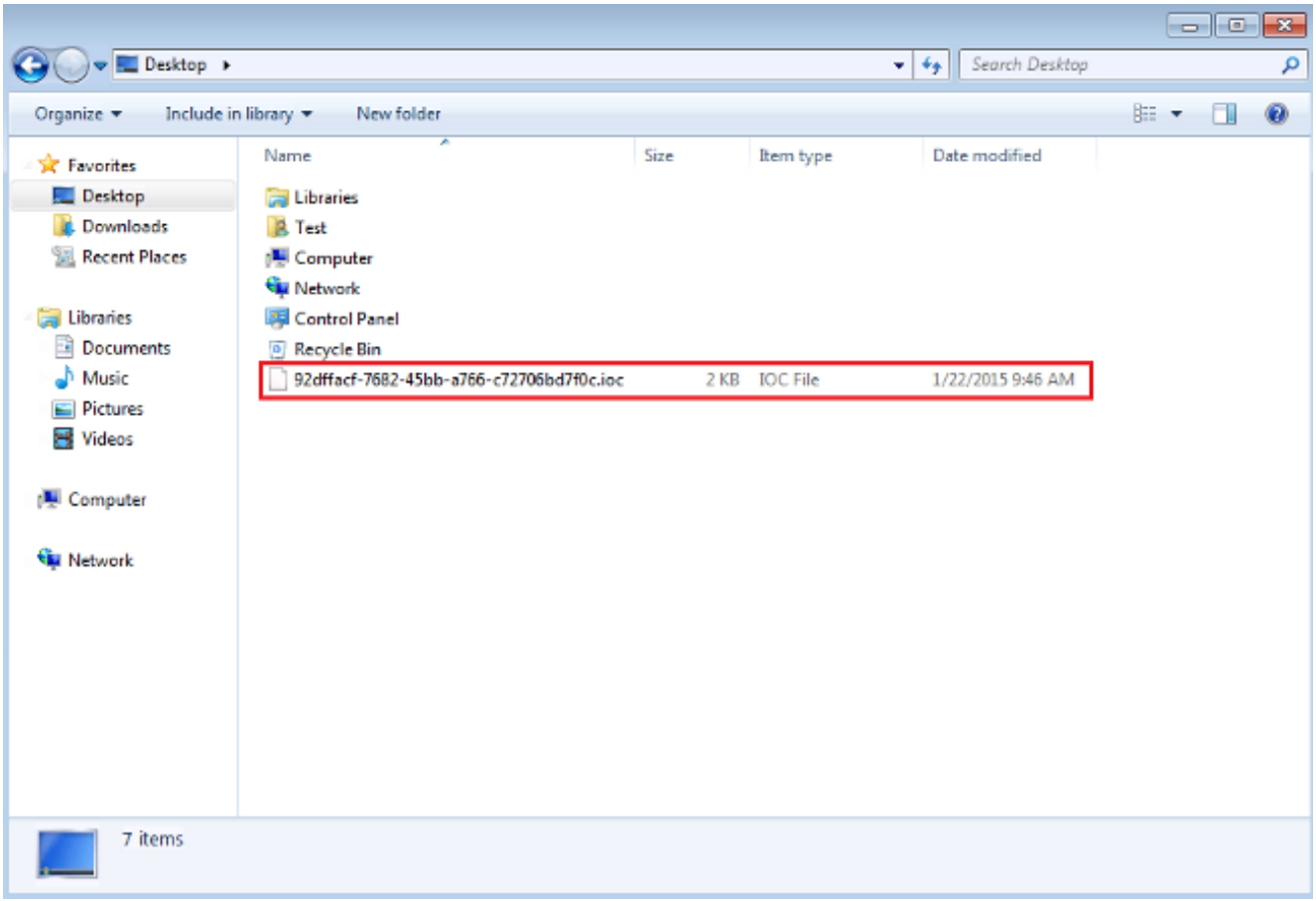
3. 등록 정보를 추가한 후 화면 오른쪽 끝에 있는 작은 아이콘을 클릭하여 구성 창을 엽니다. 이 창에서 **Content** 필드를 사용하여 파일 확장명을 일치시킵니다. 예를 들어, **test.txt** 텍스트 파일과 일치시키기 위해 txt를 추가합니다.



4. 이제 논리 연산자를 추가해야 합니다. 이 예에서는 **테스트** 텍스트 파일과 일치합니다. 이를 매칭하려면 *AND* 연산자를 사용하고 다음 속성을 추가합니다. 파일 이름을 찾아 **항목** 트리 메뉴에서 선택합니다. 속성 창에서 찾을 파일의 이름을 추가합니다. 예를 들어, Content(콘텐츠) 필드에 **테스트**를 추가합니다.



5. 이 간단한 IOC에 추가 속성이 필요하지 않으므로 파일을 저장할 수 있습니다. File(**파일**) > **Save(저장**)를 클릭하면 **.ioc** 확장자가 있는 서명 파일이 시스템에 저장됩니다.



IOC 서명 파일 업로드

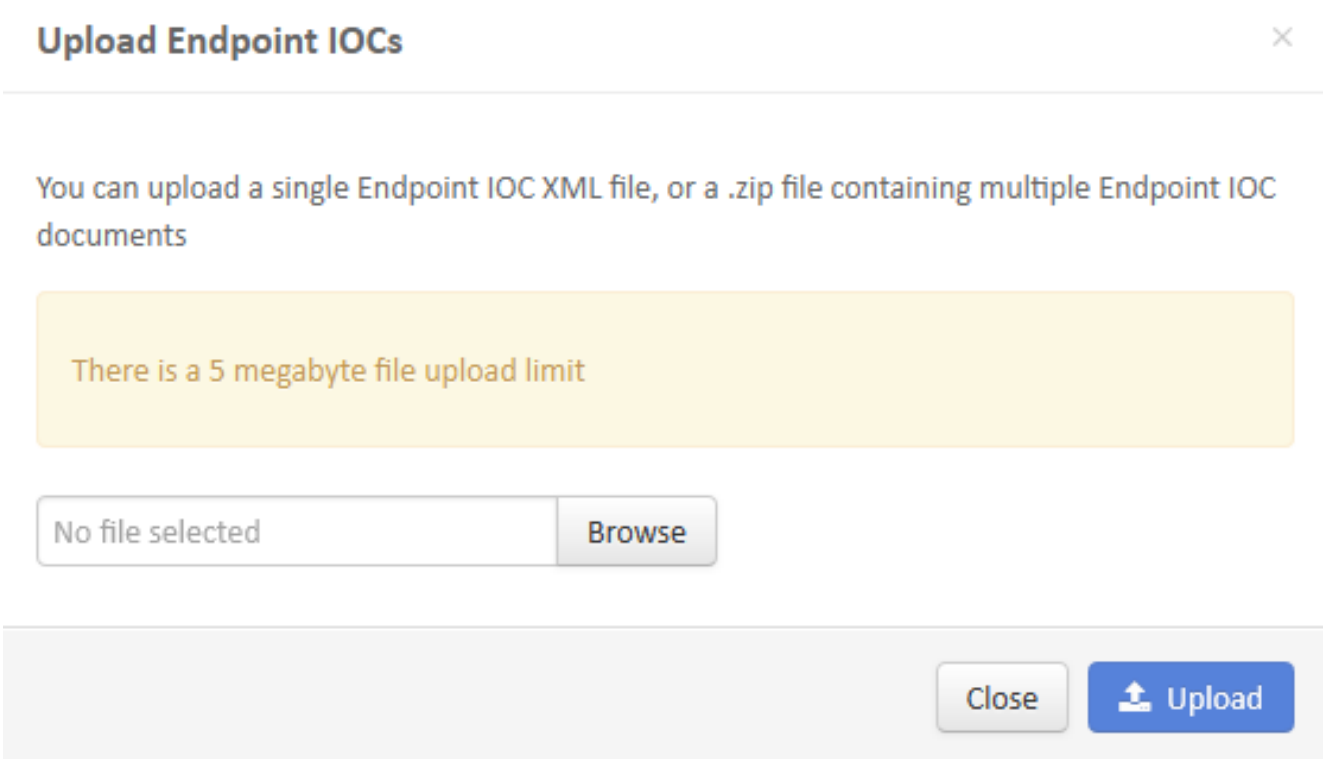
스캔을 수행하려면 IOC 파일을 FireAMP 대시보드에 업로드해야 합니다. 여러 IOC 파일을 포함하는 IOC 서명 파일, XML 파일 또는 zip 아카이브를 사용할 수 있습니다. 대시보드는 IOC 시그니처로 파일을 압축 해제하고 구문 분석합니다. 구문이 잘못되었거나 지원되지 않는 속성이 사용되면 알림이 표시됩니다.

팁: 최대 5메가바이트의 파일을 업로드할 수 있습니다.

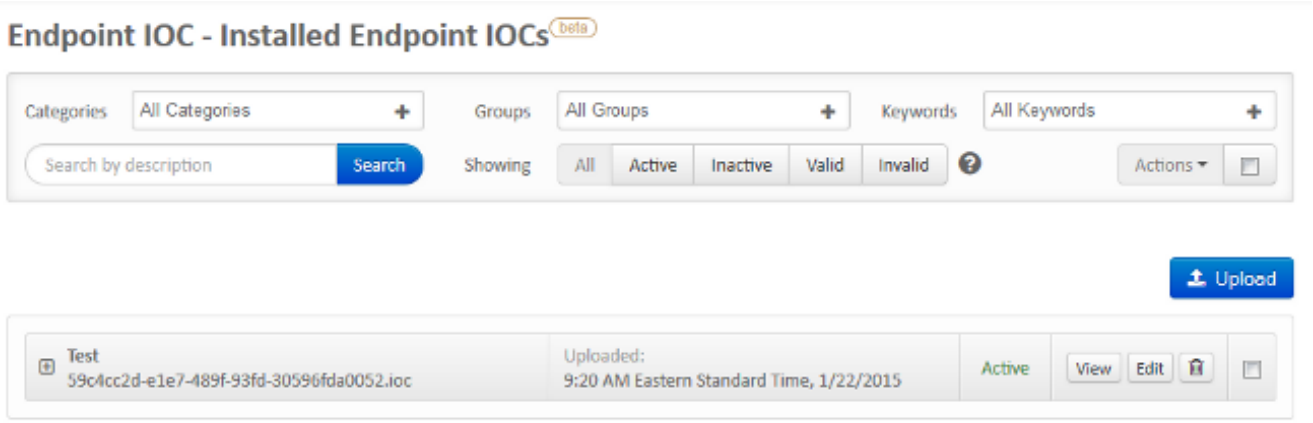
IOC 서명 파일을 FireAMP 대시보드에 업로드하려면 다음 단계를 완료하십시오.

1. FireAMP Cloud Console에 로그인하여 Outbreak Control(아웃브레이크 제어) **> Installed Endpoint IOC로 이동합니다**.

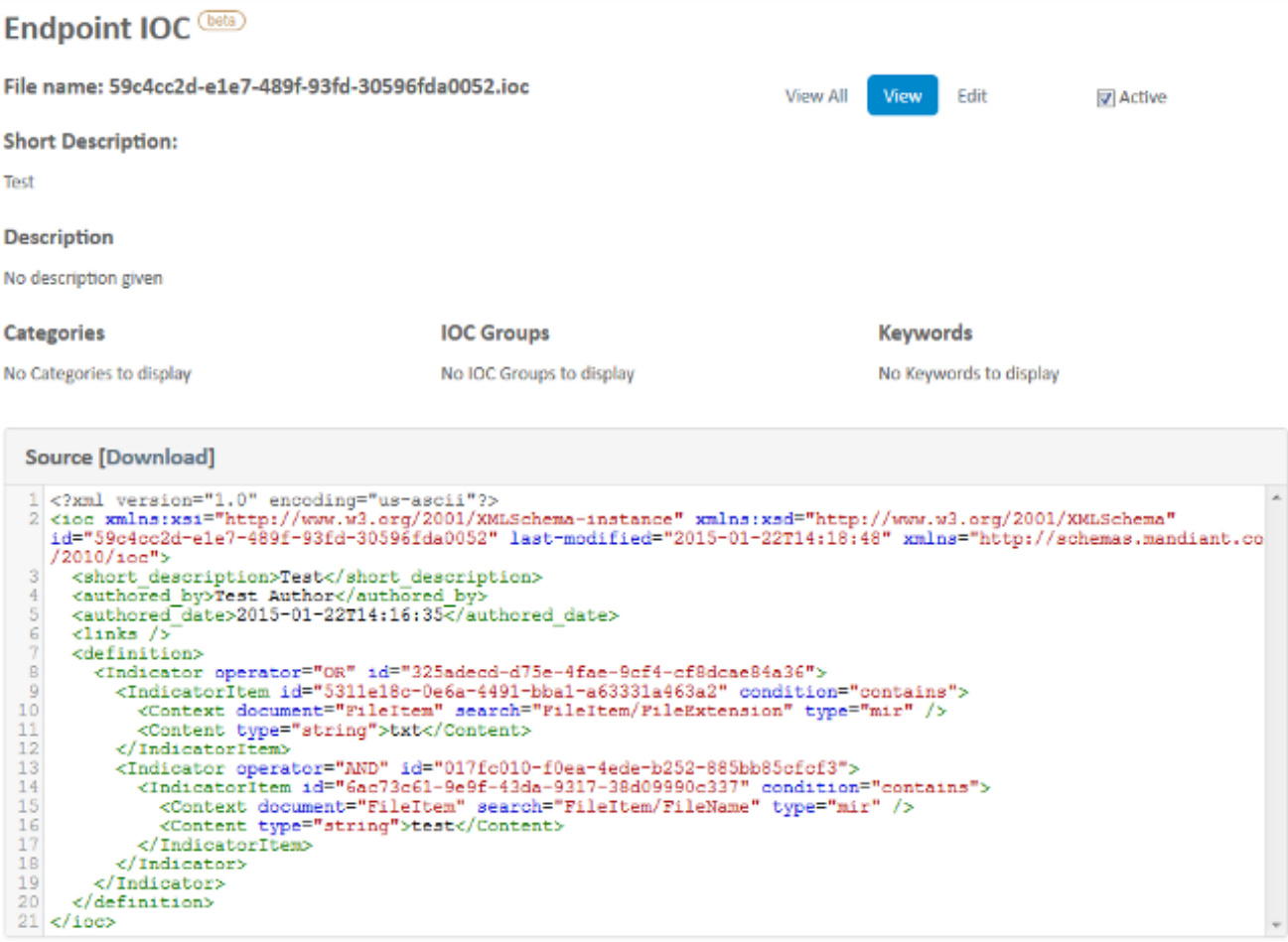
2. Upload(**업로드**)를 클릭하면 Upload Endpoint **IOCs(엔드포인트 IOC 업로드**) 창이 나타납니다.



IOC 서명 파일이 성공적으로 업로드되면 다음과 같은 서명이 목록에 나타납니다.



3. 시그니처의 실제 XML 데이터를 보려면 View를 클릭합니다.



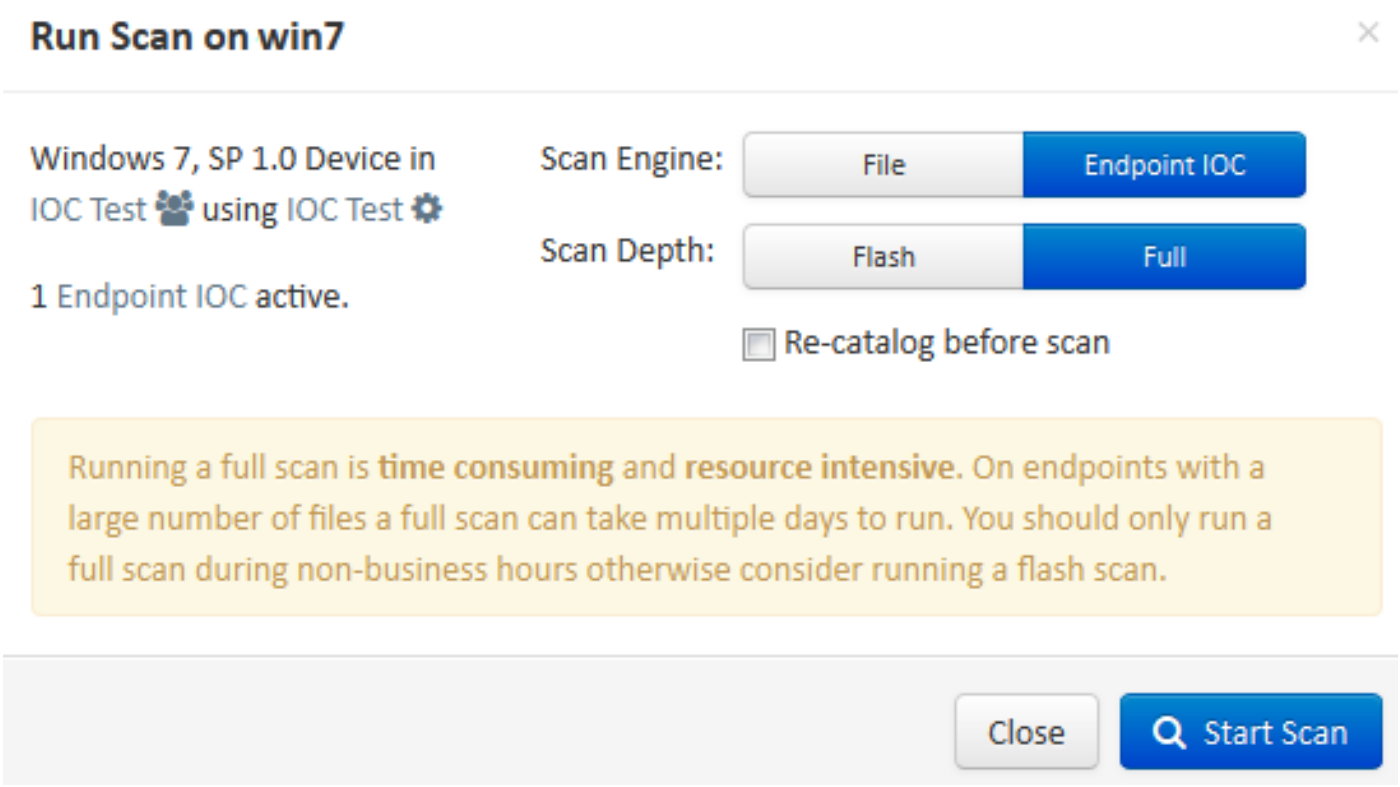
스캔 시작

서명 파일을 업로드한 후 *전체* 스캔을 수행합니다. 첫 번째 스캔은 전체 컴퓨터에 대한 메타데이터 카탈로그를 생성해야 하므로 전체 스캔이어야 합니다. 이 카탈로그는 1-2시간이 걸릴 수 있습니다. 시스템이 전체 스캔을 통해 카탈로그화된 후 *플래시* 스캔을 수행할 수 있습니다.

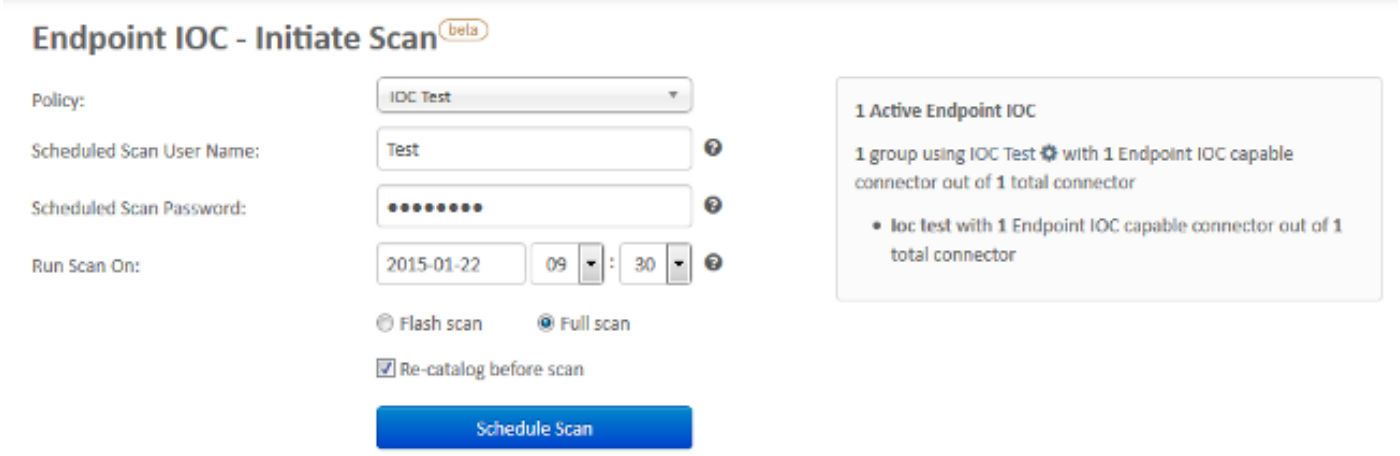
> **참고:** 전체 스캔은 CPU를 매우 많이 사용합니다. Cisco에서는 PC를 사용 중인 동안에는 전체 검사를 실행하지 않는 것이 좋습니다. 이 기능을 정기적으로 사용하려는 경우 카탈로그를 재구축하려면 한 달에 한 번 전체 스캔을 수행할 수 있습니다.

IOC 스캔을 실행하기 위해 사용할 수 있는 두 가지 방법이 있습니다. 첫 번째 방법은 이벤트 또는 대시보드에서 즉시 스캔을 수행하는 것입니다. 이는 다음에 PC가 클라우드에 하트비트를 전송할 때 트리거됩니다.

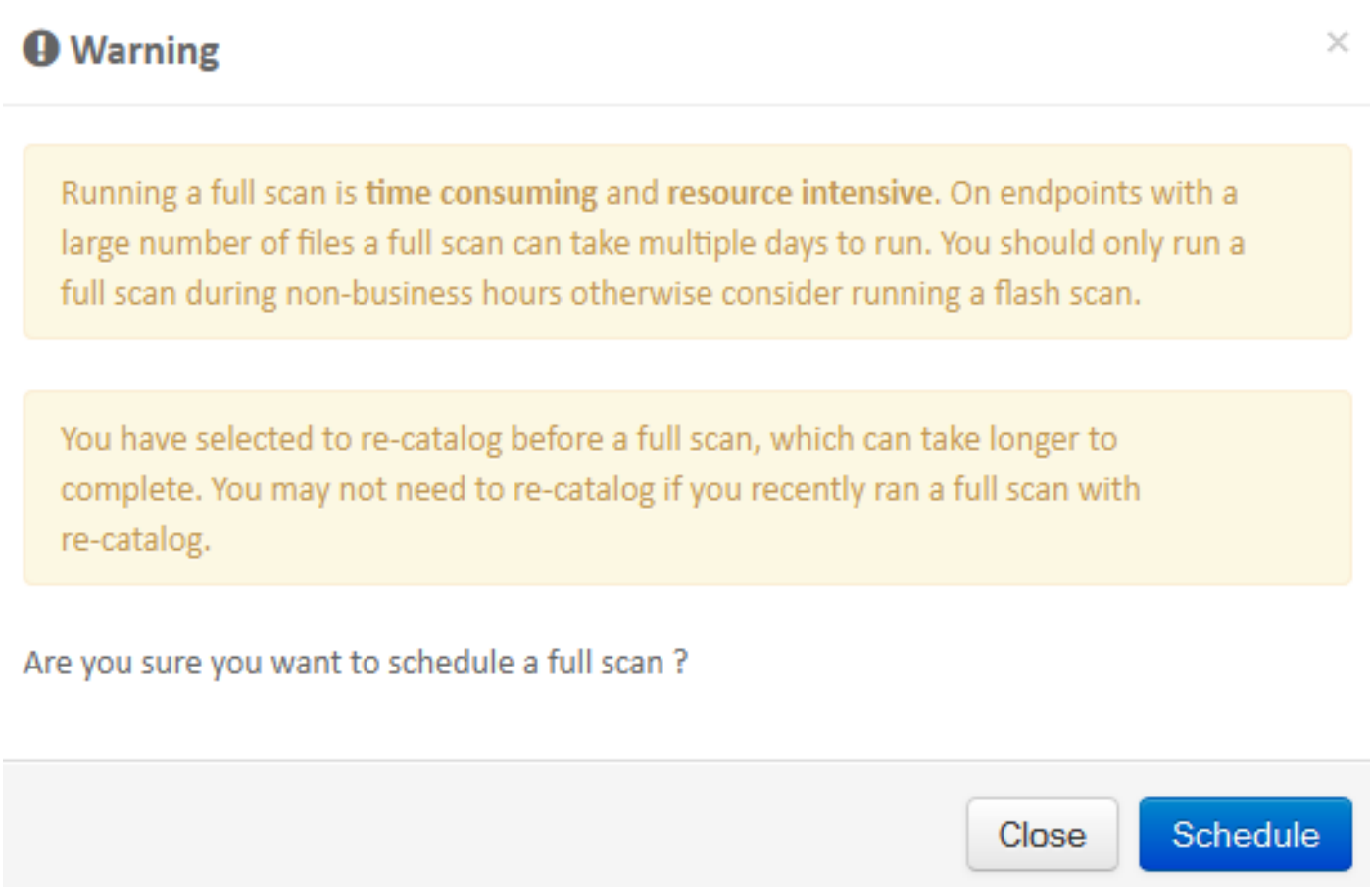
> **참고:** 전체 스캔을 처음 실행하는 경우 스캔 **전**에 **카탈로그 재작성** 옵션을 확인할 필요가 없습니다.



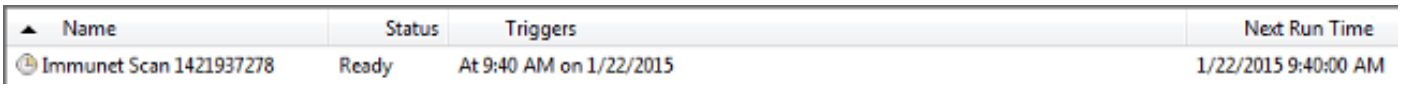
두 번째 방법은 대시보드의 Outbreak **Control** 메뉴에서 예약된 엔드포인트 IOC 스캔을 생성하는 것입니다. 이 옵션은 사용량이 적은 시간 동안 스캔을 수행하려는 경우에 적합합니다. 예약된 작업을 만들고 일괄 처리 그룹 정책 권한으로 **로그온**을 허용하려면 해당 컴퓨터에 대한 권한이 있는 계정의 자격 증명을 제공해야 합니다.



엔드포인트 IOC 스캔을 예약할 때 다음 경고 메시지가 나타납니다.

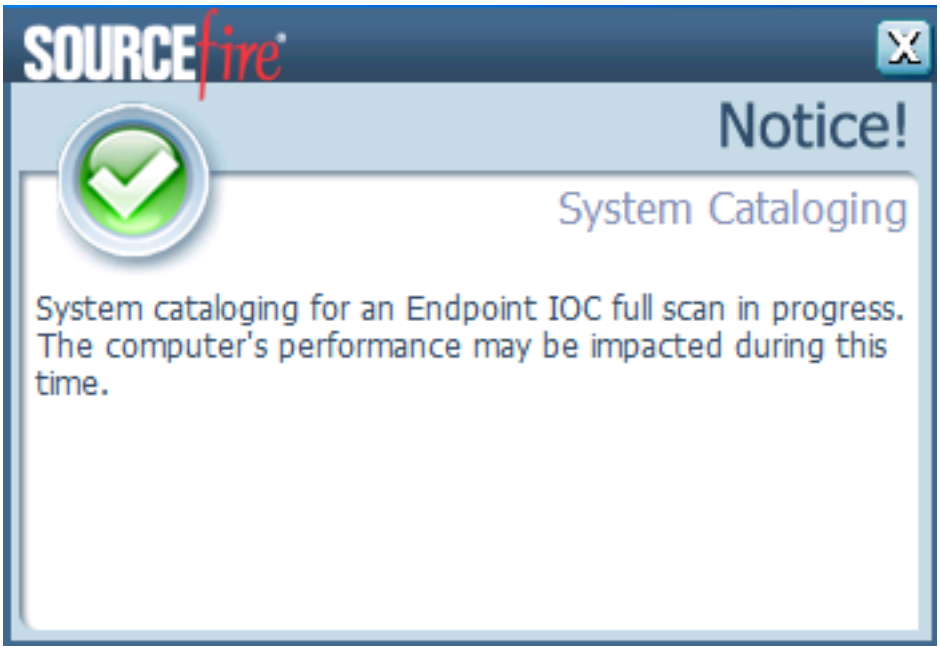


다음에 PC에서 하트비트를 전송할 때 자격 증명이 유효하면 Windows 작업 스케줄러에서 이와 유사한 작업을 볼 수 있습니다.



검사가 시작되면 다음 메시지가 나타납니다.

참고: GUI가 숨겨지도록 구성된 경우 **시스템 카탈로그 작성** 알림이 표시되지 않습니다.



스캔이 완료되면 엔드포인트 *IOC Scan Detection Summary(*엔드포인트 *IOC 스캔 탐지 요약)*를 볼 수 있습니다. 다음 예에서는 **test.txt** IOC 서명 파일에 대한 일치를 보여줍니다.