Выполните просмотры Индикации относительно компромисса (IOC) оконечной точки с AMP для оконечных точек или FireAMP

Содержание

Введение

Этот документ описывает, как создать Файл цифровой подписи Индикации относительно компромисса (IOC) через редактора IOC Mandiant, как загрузить его к информационной панели Cisco FireAMP, и как инициировать просмотр IOC оконечной точки.

Предварительные условия

Требования

Cisco рекомендует иметь по крайней мере один гигабайт свободного дискового пространства, прежде чем вы попытаетесь выполнить просмотры IOC оконечной точки.

Используемые компоненты

Сведения в этом документе основываются на сканере IOC оконечной точки, который доступен в Windows Connector Versions 4.0.2 Cisco FireAMP и позже.

Сведения, представленные в этом документе, были получены от устройств, работающих в

специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Функция сканера IOC оконечной точки является мощным программным средством реагирования на инциденты, которое используется для сканирования индикаторов посткомпромисса через несколька компьютеров.

> **Примечание:** Несмотря на то, что FireAMP поддерживает IOCS с языком Mandiant, само программное обеспечение Mandiant IOC Editor не разрабатывается или поддерживается Cisco. Поддержка Cisco не устраняет неполадки созданный пользователями или сторонний IOCS.

Файлы цифровой подписи IOC

Файл цифровой подписи IOC является расширяемой XML-схемой для описания технических характеристик, которые определяют известную угрозу, методологию атакующего или другое доказательство компромисса.

Можно импортировать IOCS оконечной точки через консоль от находящихся в OpenIOC файлов, которые записаны для включения свойств файла, таких как название, размер, и хэш, а также другие атрибуты и системные свойства, такие как информация о процессе, рабочие сервисы и Записи реестра Microsoft Windows. Синтаксис IOC может использоваться инцидентными респондентами для обнаружения определенных артефактов или для использования логики для создания сложных, коррелированых обнаружений для семейств вредоносного ПО.

Выполните просмотр на Файле цифровой подписи IOC

Существует три шага, которые необходимо выполнить для выполнения просмотра на Файле цифровой подписи IOC:

1. Создайте Файл цифровой подписи IOC.
2. Загрузите Файл цифровой подписи IOC.
3. Инициируйте просмотр.

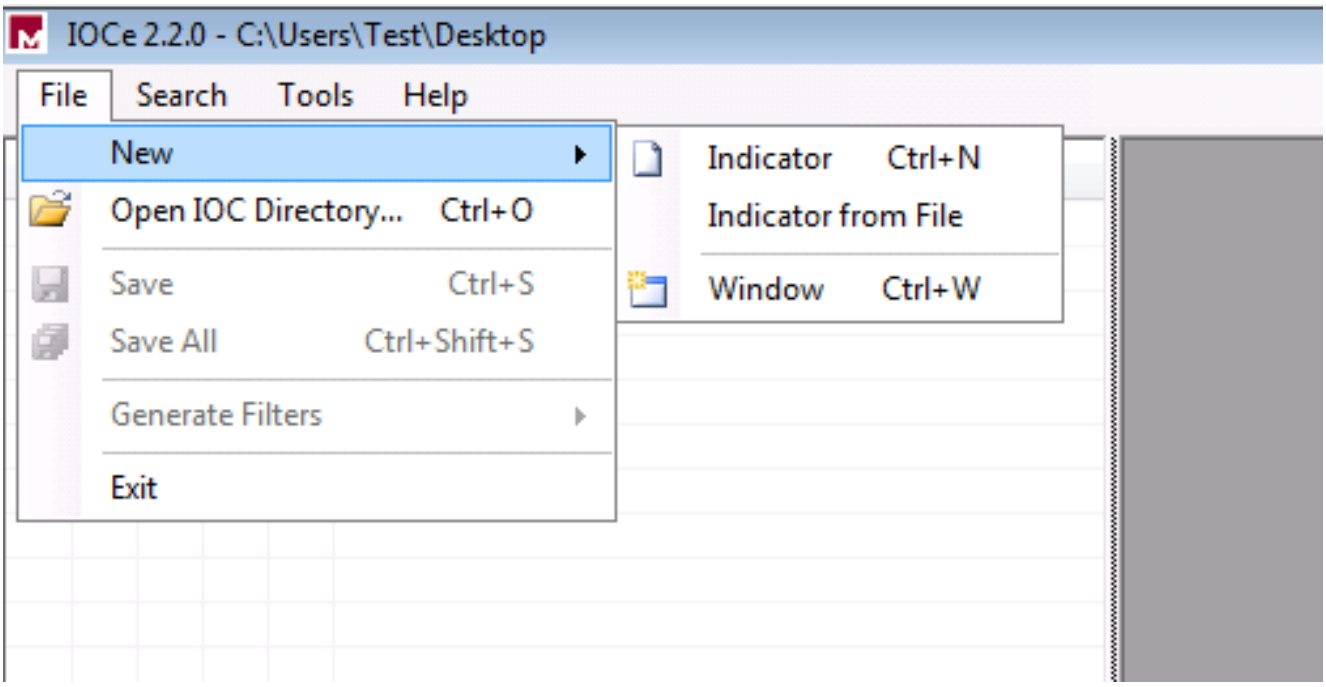
На этих шагах подробно останавливаются в разделах, которые придерживаются.

Создайте Файл цифровой подписи IOC

> **Примечание:** В данном примере редактор IOC Mandiant используется для построения Файла цифровой подписи IOC для текстового файла, названного **test.txt**.

Выполните эти шаги для создания Файла цифровой подписи IOC:

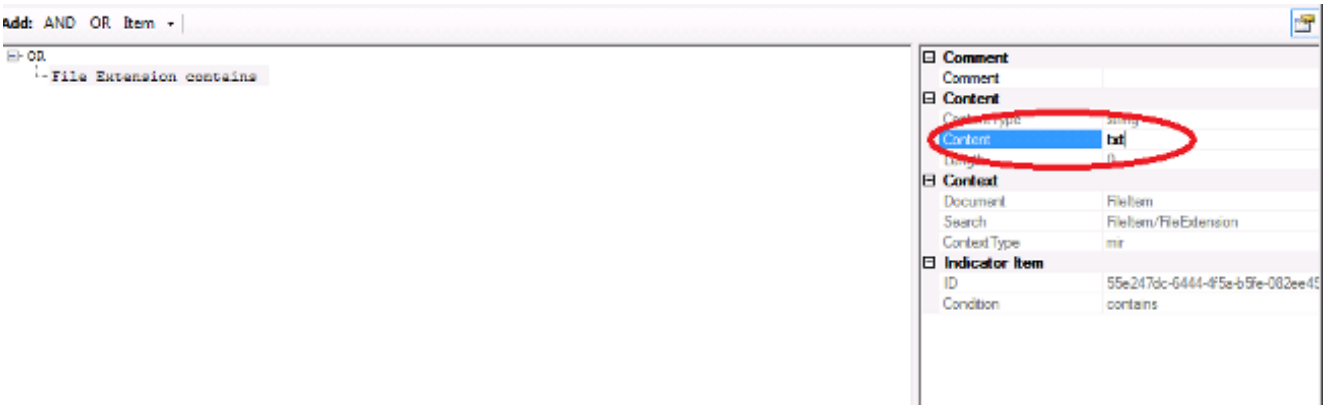
1. Откройте **IOCe** и перейдите к **Индикатору File> New>**. Это предоставляет пустую рабочую область так, чтобы можно было начать создавать IOC.



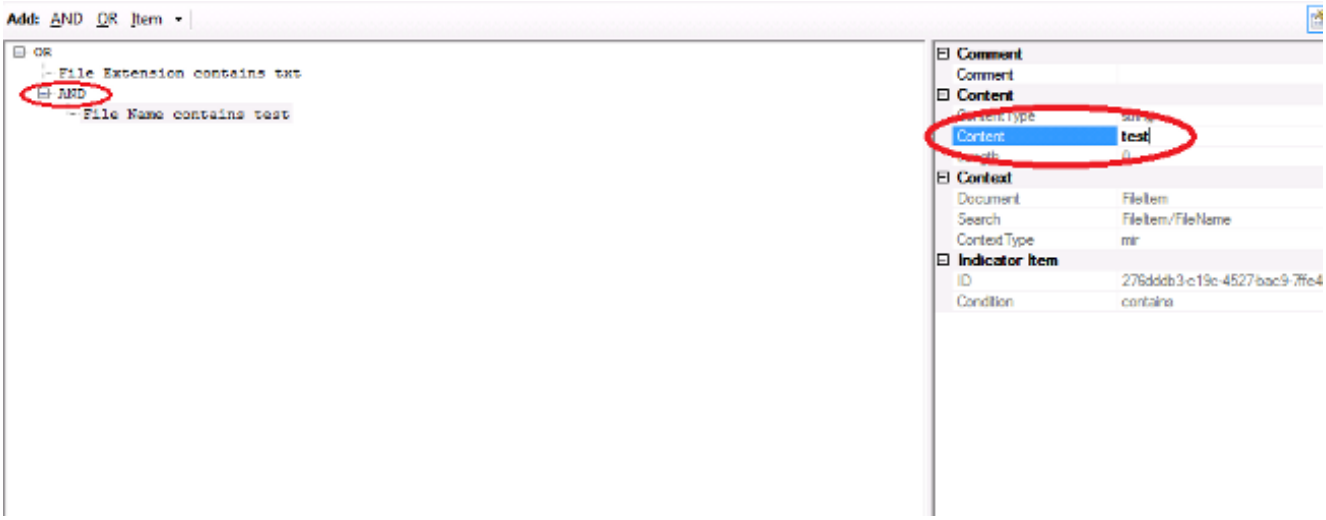
Примечание: Для создания IOC для чего-то определенного используйте бинарную логику со свойствами. Начальным оператором является OR, который является самым простым ядром для работы от. Это позволяет начальной функции IOC работать, таким образом, вы не обязаны изменять его. Требуется, что Файл цифровой подписи IOC имеет по крайней мере два свойства или условия для использования его успешно в просмотре.

2. Нажмите раскрывающееся меню **Элементов** для добавления операторов. Первым свойством, которое необходимо добавить, является **Расширение файла, содержит**. Найдите свойство в меню дерева **Элементов** и нажмите его.

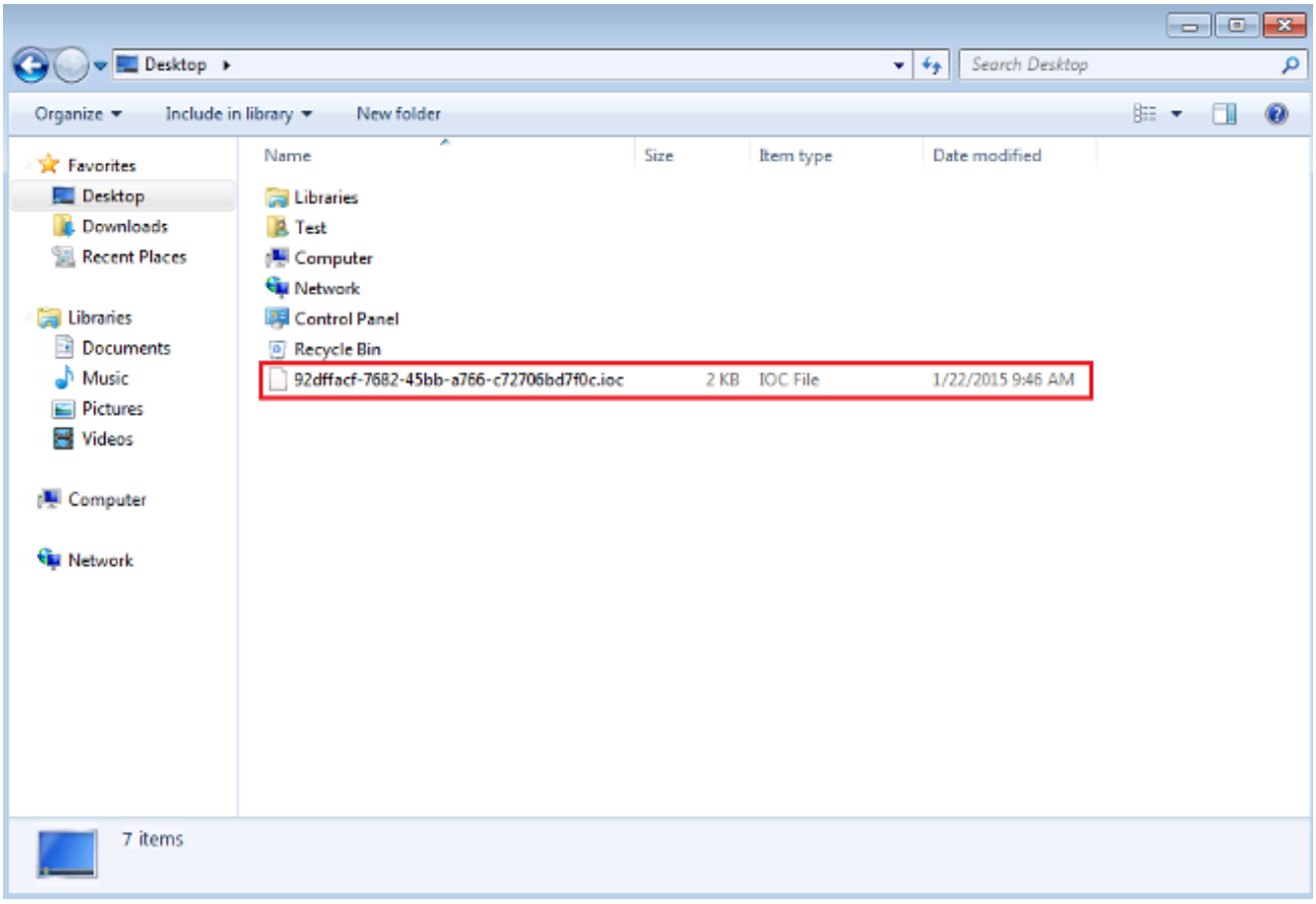
3. После добавления свойства нажмите маленький значок на дальней правой стороне экрана для открытия области Configuration. В этой области используйте поле **Content** для соответствия с расширением файла. Например, добавьте **текст** для соответствия **с test.txt** текстовым файлом:



4. Необходимо теперь добавить логический оператор. В данном примере вы будете совпадать **с тестовым** текстовым файлом. Для соответствия с этим используйте *операцию И* и добавьте следующее свойство. Найдите имя файла и выберите его из меню дерева **Элементов**. В Панели свойств добавьте название файла, который вы хотите найти. Например, добавьте **тест** в поле Content:



5. Так как никакие дополнительные свойства не необходимы для этого простого IOC, можно теперь сохранить файл. Нажмите **File> Save**, и Файл цифровой подписи с **.ioc** расширением сохранен в системе:



Загрузите Файл цифровой подписи IOC

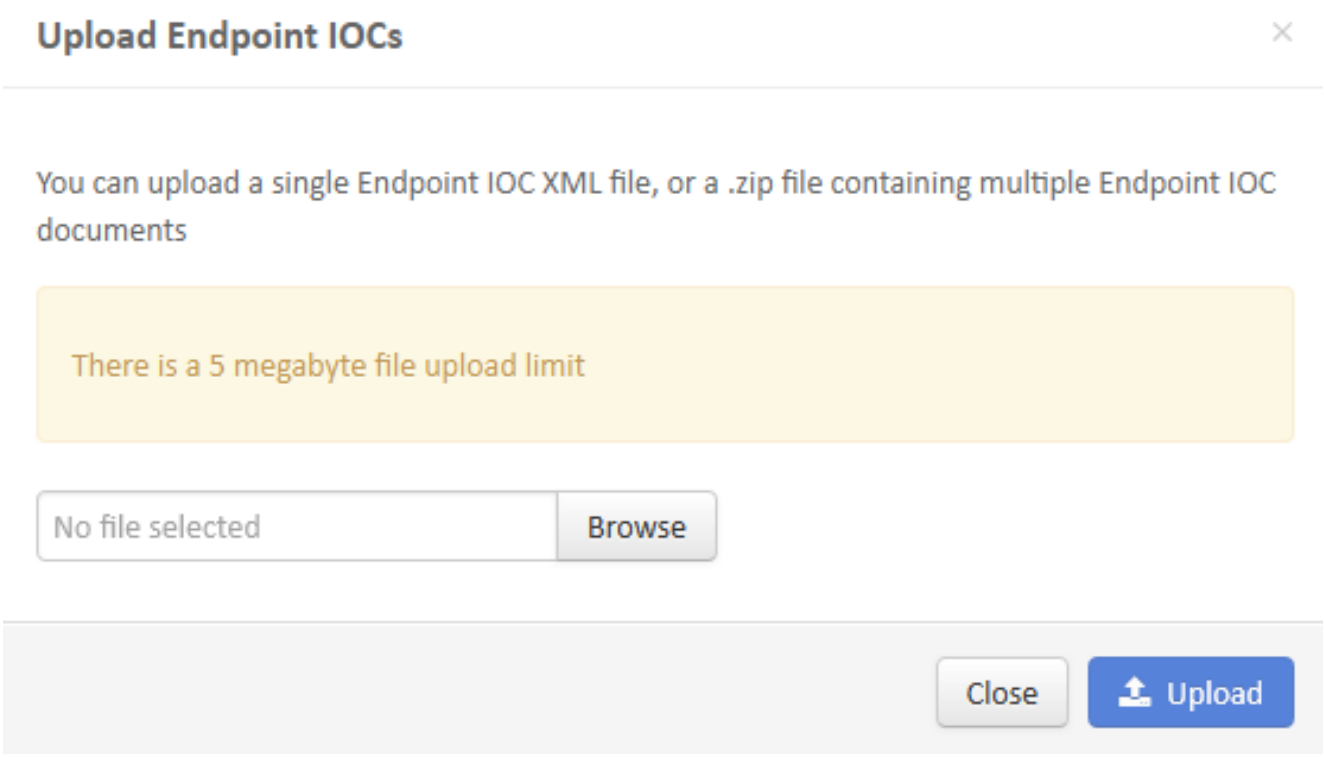
Для выполнения просмотра необходимо загрузить файл IOC к информационной панели FireAMP. Можно использовать Файл цифровой подписи IOC, XML-файл или архив zip, который содержит множественные файлы IOC. Информационная панель распаковывает и анализирует файл с подписями IOC. Если неверный синтаксис или неподдерживаемое свойство используются, вы уведомлены.

Совет: Можно загрузить файлы, которые составляют до пяти мегабайтов в размере.

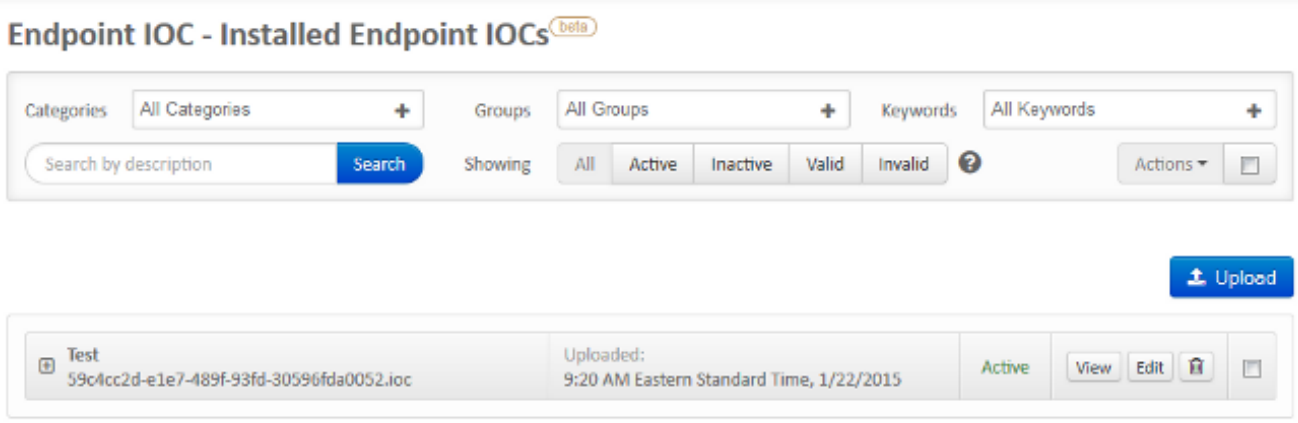
Выполните эти шаги для загрузки Файла цифровой подписи IOC к информационной панели FireAMP:

1. Войдите в Облачную Консоль FireAMP и перейдите к **Контролю за Вспышкой> Установленный IOC Оконечной точки**.

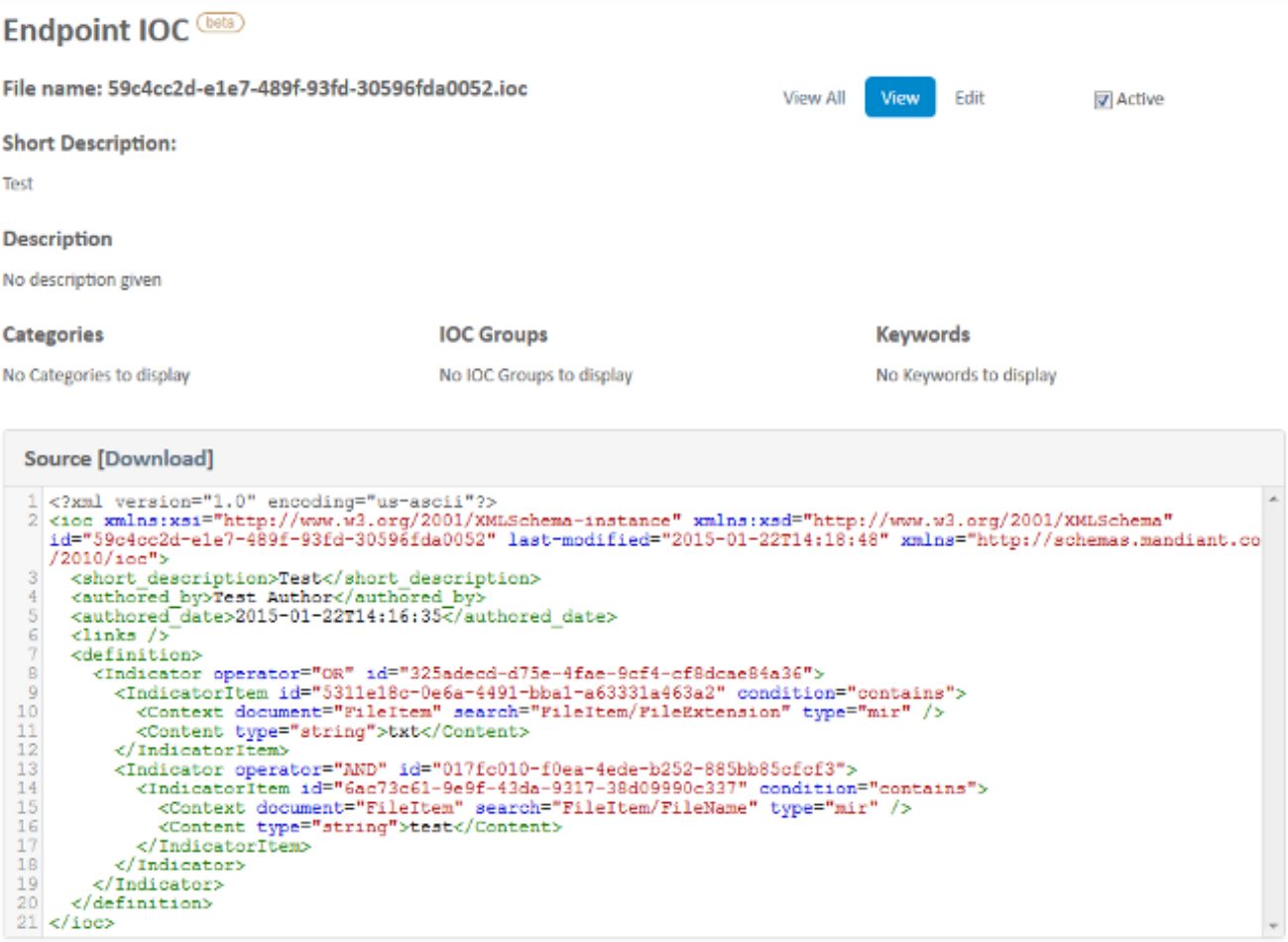
2. Нажмите **Upload**, и окно **Upload Endpoint IOCs** появляется:



После того, как Файл цифровой подписи IOC загружен успешно, подпись появляется в списке:



3. Нажмите **View** для просмотра фактических данных в XML подписи:



Инициируйте просмотр

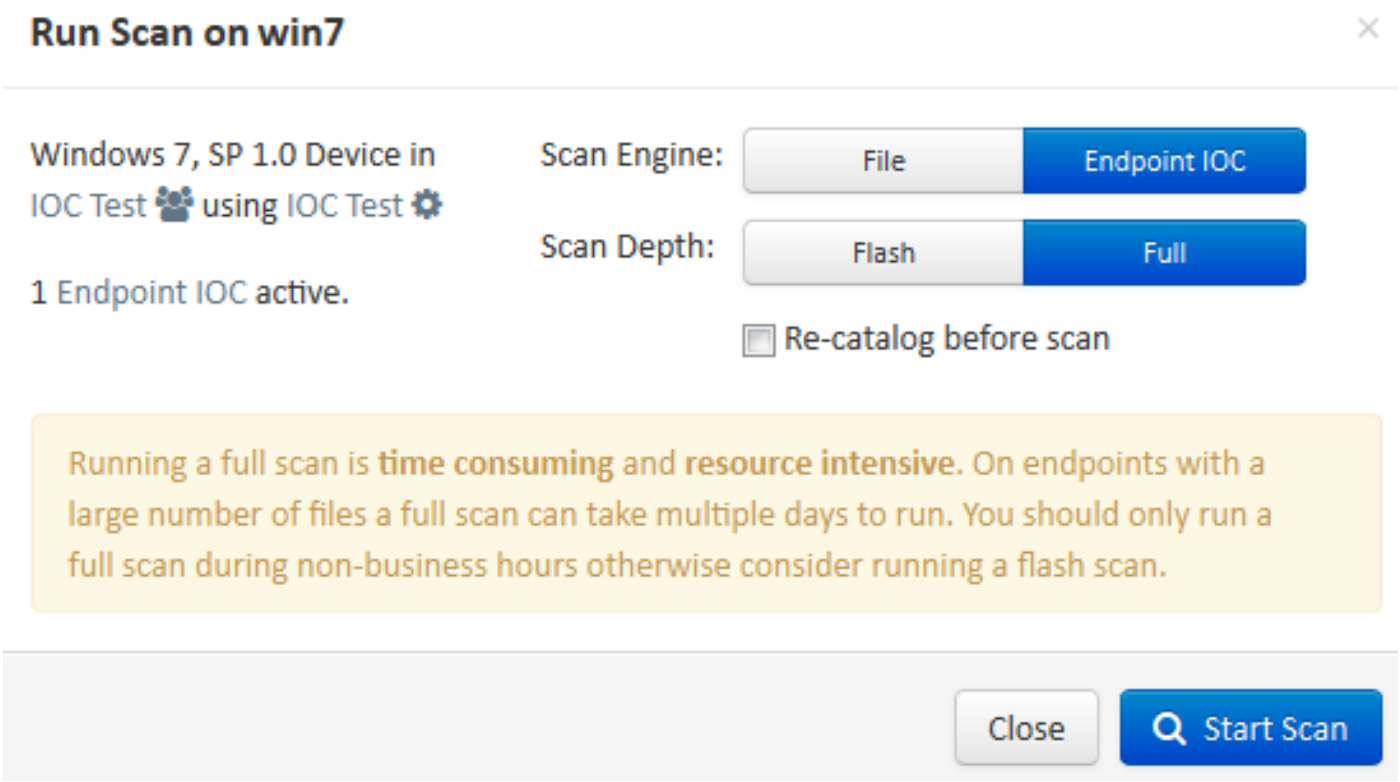
После того, как вы загружаете Файл цифровой подписи, выполняете *полный* просмотр. Первый просмотр должен быть полным просмотром, потому что он должен создать каталог метаданных для всего компьютера, который может занять 1–2 часа. Можно выполнить просмотр *флэш-памяти* после того, как система будет каталогизироваться посредством полного просмотра.

> **Примечание:** Полный просмотр является очень сом интенсивной загрузкой ЦПУ. Cisco рекомендует не выполнить полный просмотр на ПК, в то время как она используется. Если вы планируете использовать функцию регулярно, можно выполнить полный

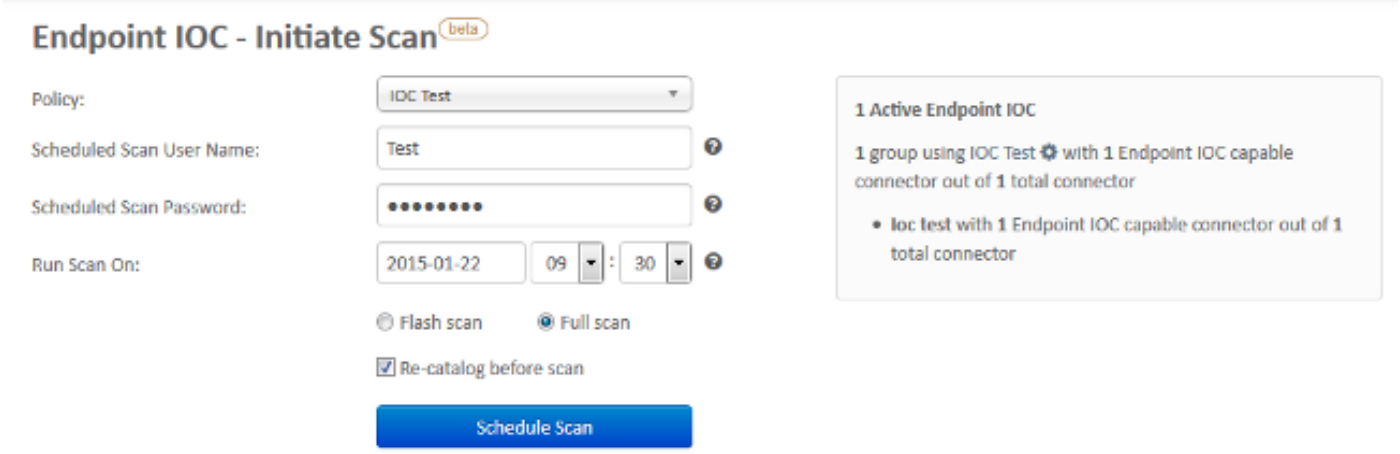
просмотр один раз в месяц для восстановления каталога.

Существует два других метода, которые можно использовать для выполнения просмотра IOC. Первый метод должен выполнить непосредственный просмотр от события или от информационной панели. Это инициировано в следующий раз, когда ПК передает биение к Облаку.

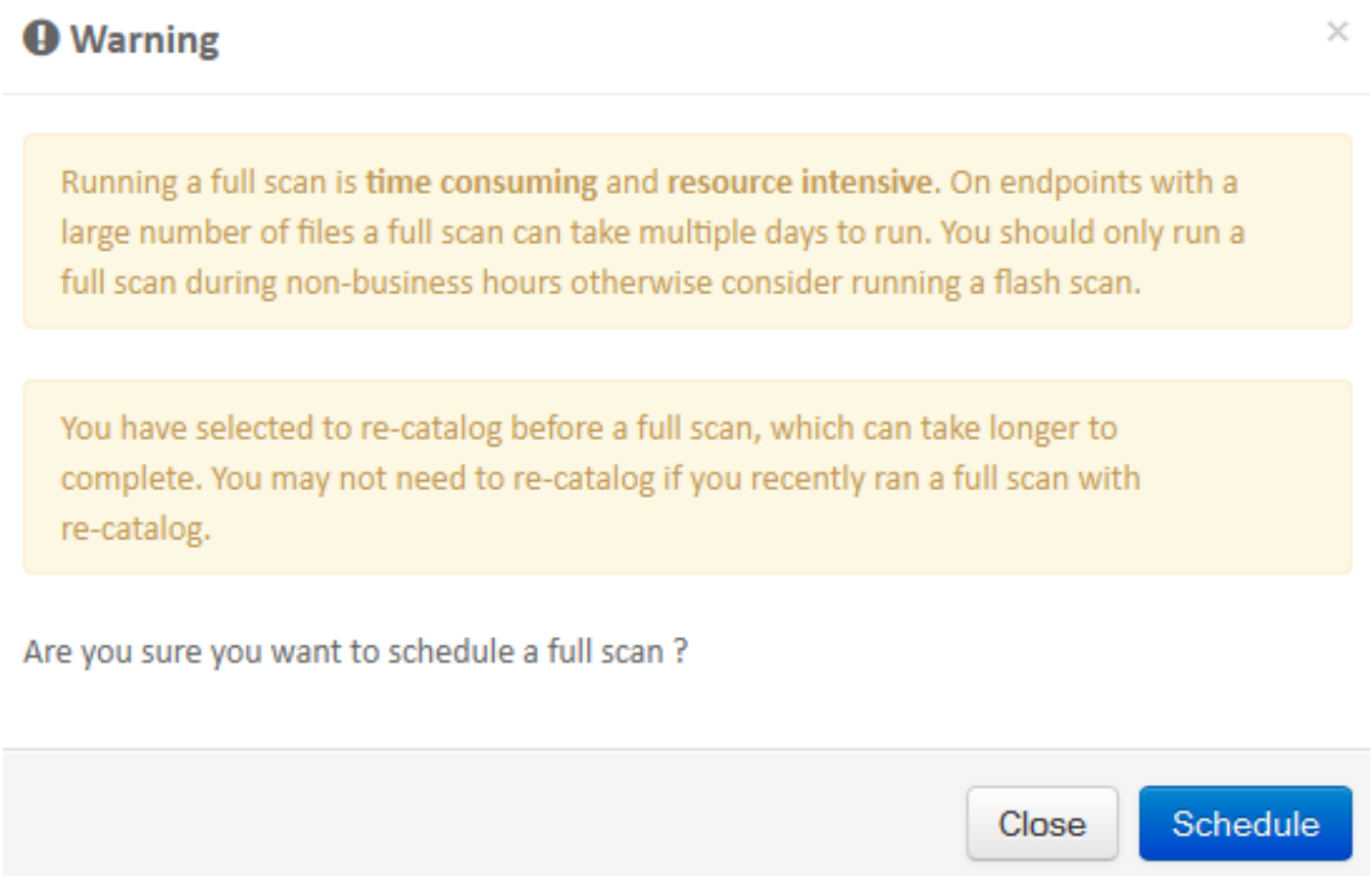
Примечание: Если это первоначально, что вы выполняете полный просмотр, вы не обязаны проверять **Перекаталог перед** опцией **просмотра**.



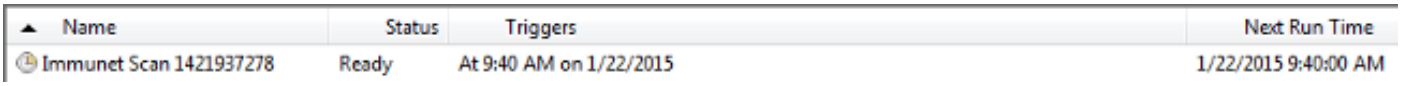
Второй метод должен создать запланированный просмотр IOC оконечной точки от **Меню управления Вспышки** информационной панели. Когда вы желаете выполнить просмотры в течение непиковый часов, эта опция могла бы быть идеальной. Необходимо предоставить учетные данные учетной записи, которая имеет разрешения на данном компьютере, чтобы создать запланированные задачи и позволить **Вход в систему как Пакетные** разрешения групповой политики.



При планировании просмотра IOC оконечной точки это предупреждающее сообщение появляется:

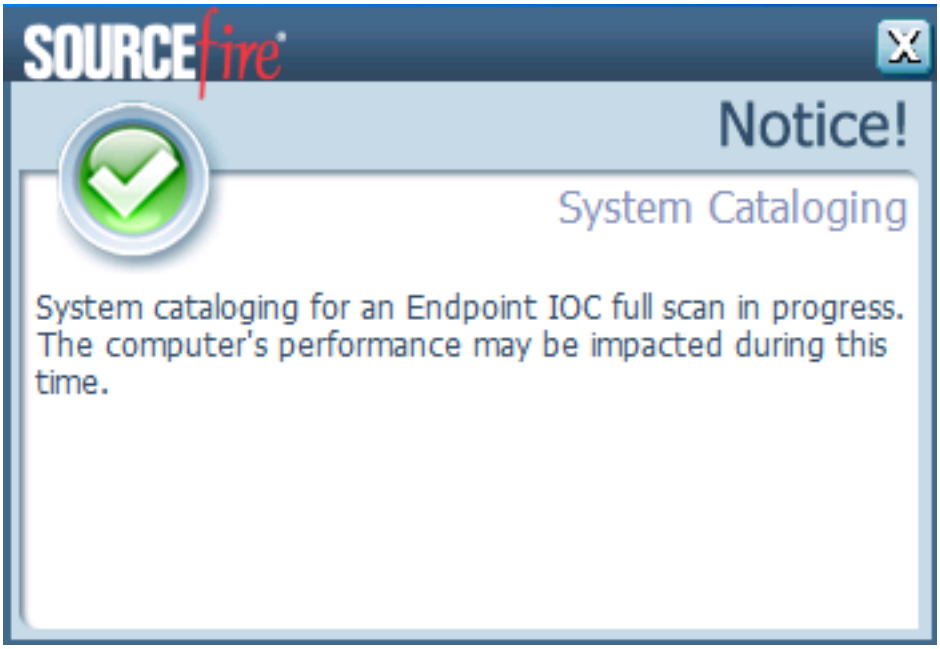


В следующий раз, когда ваш ПК передает биение, и если ваши учетные данные допустимы, необходимо видеть задание, подобное этому в Windows Task Scheduler:



Когда просмотр начинается, это сообщение появляется:

> **Примечание:** Если GUI настроен, чтобы быть скрытым, то вы не видите**, что Система Каталогизирует** предупреждение.



Когда просмотр завершен, вы в состоянии просмотреть *Сводку Обнаружения Просмотра IOC Оконечной точки*. Данный пример показывает достойный **test.txt** Файла цифровой подписи IOC: