



Sandbox

Настройка источников.
Пользовательские параметры
проверки

© Positive Technologies, 2025.

Настоящий документ является собственностью Positive Technologies и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения Positive Technologies.

Документ может быть изменен без предварительного уведомления.

Товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям.

Дата редакции документа: 24.03.2025

Содержание

1. Об этом документе	4
2. Параметры пользовательских правил (статический анализ файлов) для предварительной фильтрации... 5	
2.1. Добавление нового правила	5
2.2. Типы файлов	7
2.3. Маски имен файлов	9
2.4. Маски MIME-типов.....	11
2.5. Метки файлов.....	13
3. Параметры пользовательских правил (поведенческий анализ файлов)	16
3.1. Создание правила для исполняемых файлов Windows.....	16
3.2. Создание правила для офисных файлов, Windows	17
3.3. Создание правила для PDF-файлов, Windows.....	20
3.4. Создание правила для исполняемых файлов, Linux.....	24
3.5. Создание правила для офисных приложений, Linux	26
3.6. Создание правила для PDF-файлов, Linux	29
4. Проверка правил	34

1. Об этом документе

Документ содержит справочную информацию о действиях, выполняемых для настройки статического и поведенческого анализа в параметрах источников Positive Technologies Sandbox (далее также — PT Sandbox).

Методика адресована специалистам, выполняющим первоначальную настройку и сопровождение PT Sandbox.

2. Параметры пользовательских правил (статический анализ файлов) для предварительной фильтрации

При проверке файлов PT Sandbox выявляет различные свойства файлов и по ряду признаков устанавливает для них метки. С помощью пользовательских правил вы можете указать свойства файлов, по которым PT Sandbox будет относить их к опасным или потенциально опасным объектам. При регистрации каждого источника существует общий базовый набор правил, включенных на определение потенциально опасных объектов для подсветки подозрительного содержимого в прошедших анализ файлах.

Для более тонкой настройки предусмотрена возможность редактирования существующих и добавления собственных правил. Далее приводится методика использования таких правил.

Принцип работы правил следующий: применяются все правила по очереди, вердикт выставляется по высшему уровню опасности: если сработали правила «опасный» и «потенциально опасный», то итоговый уровень опасности объекта — «опасный».

В этом разделе

[Добавление нового правила \(см. раздел 2.1\)](#)

[Типы файлов \(см. раздел 2.2\)](#)

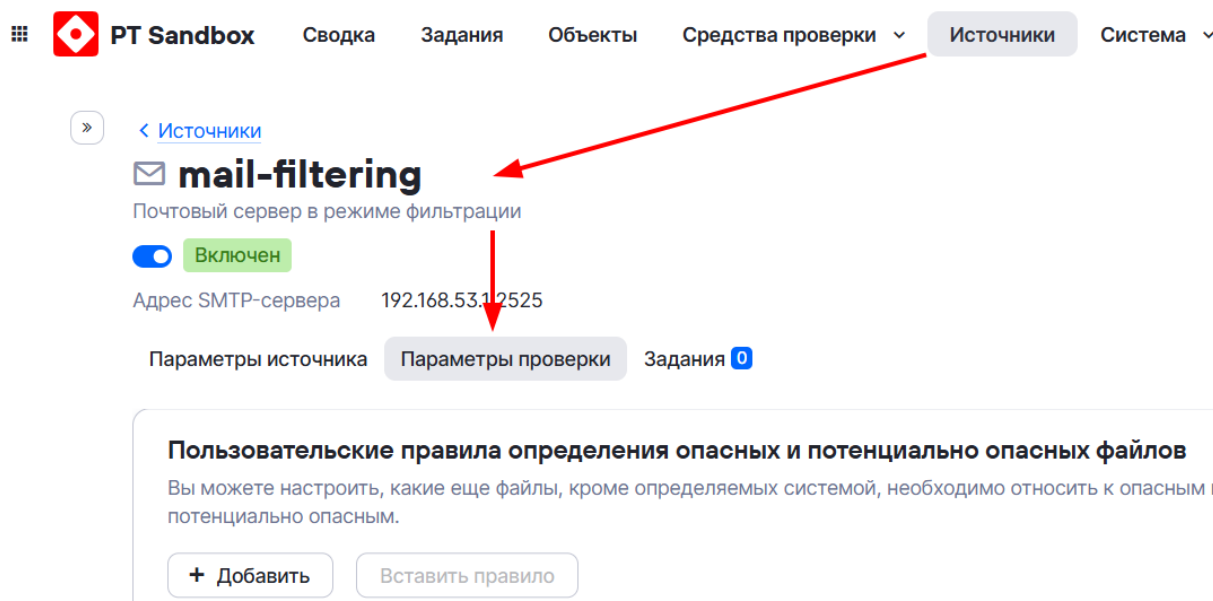
[Маски имен файлов \(см. раздел 2.3\)](#)

[Маски MIME-типов \(см. раздел 2.4\)](#)

[Метки файлов \(см. раздел 2.5\)](#)

2.1. Добавление нового правила

Для каждого регистрируемого источника (раздел **Источники**) нужно перейти на вкладку **Параметры проверки**. Здесь рассматриваются действия с блоком параметров **Пользовательские правила определения опасных и потенциально опасных файлов**.

Рисунок 1. Переход на вкладку **Параметры проверки**

После нажатия кнопки **Добавить** задается название правила и его описание. Далее определяется **Назначаемый уровень опасности**. **Опасный** применяется для большинства сценариев блокировок по вердикту, **Потенциально опасный** — для первоначальной проверки работы правила, чтобы не блокировать файлы при ложноположительных срабатываниях.

Назначаемый уровень опасности



Рисунок 2. Назначаемый уровень опасности

После определения уровня опасности задается блок параметров, которыми определяется, какие файлы **Считать опасными**. Выделено два типа правил относительно наличия у проверяемых файлов обозначенных признаков: правила прямого действия (**Только файлы со всеми указанными признаками**) и правила обратного действия (**Все файлы, кроме файлов с указанными признаками**).

Внимание! В случае правил прямого действия (**Только файлы со всеми указанными признаками**) под правило попадают файлы, которые удовлетворяют одновременно всем критериям (логическое И). Но под правила обратного действия (**Все файлы, кроме файлов с указанными признаками**) будут попадать файлы которые НЕ удовлетворяют хотя бы одному из критериев (логическое ИЛИ).

Добавление правила



Считать опасными

☒ Только файлы со всеми указанными признаками

☐ Все файлы, кроме файлов с указанными признаками

Типы файлов

▼

Маски имен файлов

Маски MIME-типов

Метки

▼

Объекты, подходящие под правило

Добавить

Отмена

Рисунок 3. Добавление нового правила

Рассмотрим несколько примеров правил с указанием различных критериев.

2.2. Типы файлов

Пример 1: мы хотим отнести к опасным все EXE-файлы, поступающие из почтового источника. Для этого в раскрывающемся списке **Типы файлов** выбираем **EXE**.

Добавление правила

X

Название

MakeExeDangerous

Может содержать только буквы латинского алфавита, цифры, дефис, точку, двоеточие, запятую, пробел, знак подчеркивания и &

Описание

Назначаемый уровень опасности

☒ Опасный ☐ Потенциально опасный

Считать опасными

- ☒ Только файлы со всеми указанными признаками
- ☐ Все файлы, кроме файлов с указанными признаками

Типы файлов

EXE X



Рисунок 4. Создание правила для EXE-файлов

Пример 2: мы хотим отнести к опасным все файлы, кроме офисных, в нашем почтовом источнике. Для этого в раскрывающемся списке **Типы файлов** выбираем **Файлы офисных приложений**.

Добавление правила



Название

PassOnlyOfficeFiles

Может содержать только буквы латинского алфавита, цифры, дефис, точку, двоеточие, запятую, пробел, знак подчеркивания и &

Описание

Назначаемый уровень опасности

☒ Опасный ☐ Потенциально опасный

Считать опасными

- ☐ Только файлы со всеми указанными признаками
- ☒ Все файлы, кроме файлов с указанными признаками

Типы файлов

Файлы офисных приложений ×



Рисунок 5. Создание правила для файлов офисных приложений

2.3. Маски имен файлов

Пример 3: рассмотрим сценарий, когда мы получаем имена вредоносных файлов из TI-отчета и хотим пометить их в качестве опасных.

Добавление правила

✕

Название

Forbid exe files if name contains malware

Может содержать только буквы латинского алфавита, цифры, дефис, точку, двоеточие, запятую, пробел, знак подчеркивания и &

Описание

Назначаемый уровень опасности

☒ Опасный ☐ Потенциально опасный

Считать опасными

- ☒ Только файлы со всеми указанными признаками
- ☐ Все файлы, кроме файлов с указанными признаками

Типы файлов

EXE ✕



Маски имен файлов

malware ✕

Маски MTMF-типов

Рисунок 6. Создание правила для имен вредоносных файлов

Пример 4: отмечаем опасными все файлы, кроме тех исполняемых файлов, которые приходят нам с соответствующей пометкой от системы передачи файлов, — или кроме тех, которые содержат определенный постфикс в названии файла.

Добавление правила



Название

Allow only executable files if name contains mask

Может содержать только буквы латинского алфавита, цифры, дефис, точку, двоеточие, запятую, пробел, знак подчеркивания и &

Описание

Назначаемый уровень опасности

☒ Опасный ☐ Потенциально опасный

Считать опасными

- ☐ Только файлы со всеми указанными признаками
- ☒ Все файлы, кроме файлов с указанными признаками

Типы файлов

Исполняемые файлы ×



Маски имен файлов

_allowed ×

Рисунок 7. Создание правила для файлов с определенным постфиксом в названии

2.4. Маски MIME-типов

Пример 5: запрет по маске MIME-типа (обратите внимание на звездочку в конце: для работы маски она необходима).

Добавление правила

Название

Forbid mime type mask

Может содержать только буквы латинского алфавита, цифры, дефис, точку, двоеточие, запятую, пробел, знак подчеркивания и &

Описание

Назначаемый уровень опасности

☒ Опасный ☐ Потенциально опасный

Считать опасными

- ☒ Только файлы со всеми указанными признаками
☐ Все файлы, кроме файлов с указанными признаками

Типы файлов

Маски имен файлов

Маски MIME-типов

application/vnd.microsoft.portable-executable* ×

application/x-dosexec* ×

Рисунок 8. Создание правила с запретом по маске MIME-типа

Также маски MIME-типов могут быть полезны, когда нужно запретить (разрешить) подмножество форматов файлов, например определенные стандарты PDF-файлов, а не весь тип. И еще более важной может быть необходимость запретить (разрешить) файлы тех форматов, для которых нет определяемого типа файла.

2.5.Метки файлов

Перед тем как выполнять следующие шаги, обязательно ознакомьтесь с перечнем определяемых PT Sandbox [меток объектов](#), который приведен в Справке специалиста по безопасности.

Последний критерий — **Метки**. В общем случае можно воспользоваться исходными правилами с метками, которые установлены по умолчанию.

Добавление правила



Считать опасными

☒ Только файлы со всеми указанными признаками

☐ Все файлы, кроме файлов с указанными признаками

▼ ☐ Все метки (25)

- ☐ Архив
- ☐ Сжатый файл
- ☐ Зашифрованный
- ☐ Многотомный
- ☐ Письмо
- ☐ SFX
- ☐ SFX ACE

Объекты, подходящие под правило

Добавить **Отмена**

Рисунок 9. Список исходных правил с метками

Примерами здесь служат наборы базовых правил: PDF с Action (действиями), PDF со встроенными объектами (OLE), PDF с JavaScript-кодом, PDF с OpenAction (действия при открытии файла).

☒ pdf.hasAction			
Назначаемый уровень оп...	Считать опасными	Типы файлов	Метки
☒ Потенциально опасный	Только файлы со всеми указанными признаками	Файлы PDF	Содержит Action

☒ pdf.hasEmbedded			
Назначаемый уровень оп...	Считать опасными	Типы файлов	Метки
☒ Потенциально опасный	Только файлы со всеми указанными признаками	Файлы PDF	Со встроенными объектами

☒ pdf.hasJavascript			
Назначаемый уровень оп...	Считать опасными	Типы файлов	Метки
☒ Потенциально опасный	Только файлы со всеми указанными признаками	Файлы PDF	Содержит JavaScript

☒ pdf.hasOpenAction			
Назначаемый уровень оп...	Считать опасными	Типы файлов	Метки
☒ Потенциально опасный	Только файлы со всеми указанными признаками	Файлы PDF	Содержит OpenAction

Рисунок 10. Наборы базовых правил

После применения созданных наборов правил следует какое-то время пронаблюдать за их работой и регулярно отслеживать их актуальность и применимость.

При наличии настроенного набора правил можем перейти к использованию опции **Прекращать проверку для всего задания** — в зависимости от красного («опасный») или желтого («потенциально опасный») вердикта. Включение этих опций позволяет экономить производительность системы путем остановки проверки на этапе статического анализа. По умолчанию обе опции выключены. Рассмотрим случаи, когда нужно их включение.

Прекращать проверку для всего задания

- ☐ Если обнаружен опасный файл
- ☐ Если обнаружен потенциально опасный файл

Рисунок 11. Опции прекращения проверки для всего задания

Первый вариант **Если обнаружен опасный файл** может быть отключен в случаях, когда требуется исследовать образцы с источника подробно, даже если уже обнаружен опасный файл (например, для тестирования работы PT Sandbox). В остальных случаях — включаем.

Второй вариант **Если обнаружен потенциально опасный файл** может быть включен, если есть потребность блокировать задания даже в случае нахождения потенциально опасных файлов.

Если правила статического анализа на этом этапе проверки срабатывают, то поведенческий анализ не запускается.

Далее переходим к пользовательским правилам поведенческого анализа.

3. Параметры пользовательских правил (поведенческий анализ файлов)

В этом блоке выполняется настройка основного инструмента из набора экспертизы PT Sandbox — включение обработки и определение параметров проверки файлов на выбранных образах операционных систем.

В этом разделе

[Создание правила для исполняемых файлов Windows \(см. раздел 3.1\)](#)

[Создание правила для офисных файлов, Windows \(см. раздел 3.2\)](#)

[Создание правила для PDF-файлов, Windows \(см. раздел 3.3\)](#)

[Создание правила для исполняемых файлов, Linux \(см. раздел 3.4\)](#)

[Создание правила для офисных приложений, Linux \(см. раздел 3.5\)](#)

[Создание правила для PDF-файлов, Linux \(см. раздел 3.6\)](#)

3.1. Создание правила для исполняемых файлов Windows

Начальное разделение параметров запуска — по семействам операционных систем (Windows и GNU/Linux). Для этого опираемся на наиболее распространенные в инфраструктуре ОС и включаем в PT Sandbox поддерживаемые, список которых можно найти в Справке оператора безопасности.

В качестве первого примера набора правил рассмотрим настройку для семейства Windows, из которого выберем образ Windows 10-1803.

Первым настроим правило проверки на следующие **Типы проверяемых файлов**: исполняемые (приложения и системные) файлы.

Продолжительность наблюдения за файлом — 4 минуты (в принципе это значение можно увеличивать или уменьшать в зависимости от имеющихся аппаратных ресурсов, объема файлов и скорости их передачи). Если опираться на то, что мы настраиваем проверку почтового типа источника, то исполняемых файлов должно будет быть меньше, чем документов, и много ресурса проверки они не займут.

Расшифровывать и анализировать HTTPS-трафик в данном случае рекомендуется, чтобы сетевые правила могли отловить вредоносную активность в зашифрованном трафике.

Изменение правила



Название

Executables Windows

Образ виртуальной машины

win10-1803-x64 (Microsoft Windows 10 Pro 1803 x64)

Файлы будут проверяться в виртуальной машине, развернутой из этих образов

Типы проверяемых файлов

Файлы приложений x

Исполняемые файлы x

Системные файлы x



Чем больше типов, тем больше может быть очередь файлов на проверку

Продолжительность наблюдения за файлом

4

минуты

0

секунд

По истечении этого времени анализ файла будет прерван с сохранением результатов

☒ Расшифровывать и анализировать HTTPS-трафик

☐ Отключить запись видео

[Объекты, подходящие под правило](#)

Изменить

Отмена

Удалить

Рисунок 12. Создание правила для исполняемых файлов Windows

3.2. Создание правила для офисных файлов, Windows

Вторым настроим правило проверки на следующие **Типы проверяемых файлов**: файлы, которые обычно открываются офисным пакетом ПО.

Добавление правила

x

Название

Office files

Образ виртуальной машины

win10-1803-x64 (Microsoft Windows 10 Pro 1803 x64)

Файлы будут проверяться в виртуальной машине, развернутой из этих образов

Типы проверяемых файлов

Документы x Презентации x Таблицы x PUB x еще 1 x v

🔍 |

- ▼ ☒ Файлы офисных приложений
 - > ☒ Документы
 - > ☒ Презентации
 - > ☒ Таблицы
 - ☐ PDF
 - ☒ PUB
- ▼ ☒ Файлы данных
 - ▼ ☒ Табличные данные

Рисунок 13. Создание правила для офисных файлов, Windows

Для этих файлов далее обратим внимание на определенные песочницей **Метки**.

Добавление правила

>

Файлы будут проверяться в виртуальной машине, развернутой из этих образов

Типы проверяемых файлов

Документы × Презентации × Таблицы × PUB × еще 1 × ▾

Чем больше типов, тем больше может быть очередь файлов на проверку

Файлы офисных форматов

☐ Все

☒ Только

С макросами Со встроенными объектами С элементами ActiveX

С запросами к внешним данным Использующие шаблон ▾

С функциями DDE С настроенными действиями (Actions)

С надстройками Office

☐ Зашифрованные

☒ С макросами

☒ Со встроенными объектами

☒ С элементами ActiveX

☒ С запросами к внешним данным

☒ Использующие шаблон

☒ С функциями DDE

☒ С настроенными действиями (Actions)

Рисунок 14. Добавление меток

Как правило, в поведенческом анализе есть смысл запускать файлы, метки в которых указывают на наличие активного содержимого. Это практически весь список, кроме метки **Зашифрованные**. Запуск файлов с такой меткой остается опциональным и зависит от политик ИБ в организации, но в общей практике его рекомендуется включить. **Продолжительность наблюдения за файлом**: если мы определяем проверку только объектов с метками (с точки зрения экономии ресурса поведенческого анализа) — выбираем 3 минуты.

Изменение правила

x

Название

Office files Windows

Образ виртуальной машины

win10-1803-x64 (Microsoft Windows 10 Pro 1803 x64)

Файлы будут проверяться в виртуальной машине, развернутой из этих образов

Типы проверяемых файлов

PUB x

Документы x

Презентации x

Таблицы x

еще 1 x



Чем больше типов, тем больше может быть очередь файлов на проверку

Файлы офисных форматов

☐ Все

☒ Только

С макросами

Со встроенными объектами

С элементами ActiveX

С запросами к внешним данным

Использующие шаблон

С функциями DDE

С настроенными действиями (Actions)

С надстройками Office

Зашифрованные



Рисунок 15. Выбор продолжительности наблюдения за файлом

3.3. Создание правила для PDF-файлов, Windows

Третье правило — по оставшемуся типу PDF.

Добавление правила



Название

PDF Windows

Образ виртуальной машины

win10-1803-x64 (Microsoft Windows 10 Pro 1803 x64)

Файлы будут проверяться в виртуальной машине, развернутой из этих образов

Типы проверяемых файлов

PDF x

PDF

- > ☐ Системные файлы ⚠
- ✓ ☒ Файлы офисных приложений
 - > ☐ Документы ⚠
 - > ☐ Презентации ⚠
 - > ☐ Таблицы ⚠
 - ☒ PDF
 - ☐ PUB ⚠
- > ☐ Файлы данных ⚠

Рисунок 16. Создание правила для PDF-файлов, Windows

Для этих файлов далее также обратим внимание на определенные песочницей **Метки**.

Добавление правила



название

PDF Windows

Образ виртуальной машины

win10-1803-x64 (Microsoft Windows 10 Pro 1803 x64)

Файлы будут проверяться в виртуальной машине, развернутой из этих образов

☐ Зашифрованные

☒ Со сценариями JavaScript

☒ С настроенными действиями при открытии (OpenActions)

☒ С настроенными действиями (Actions)

☒ Со встроенными объектами

☐ Защищенные

Со сценариями JavaScript

С настроенными действиями при открытии (OpenActions)

С настроенными действиями (Actions)

Со встроенными объектами

Продолжительность наблюдения за файлом

Рисунок 17. Добавление меток

Отмечаем в раскрывающемся списке все, кроме меток **Зашифрованные** и **Защищенные**. Запуск файлов с такими метками остается опциональным и зависит от политик ИБ в организации, но в общей практике его рекомендуется включить. Продолжительность: если мы определяем проверку только объектов с метками (с точки зрения экономии ресурса поведенческого анализа) — выбираем 2 минуты.

Изменение правила



Файлы будут проверяться в виртуальной машине, развернутой из этих образов

Типы проверяемых файлов

PDF  

Чем больше типов, тем больше может быть очередь файлов на проверку

Файлы PDF

☐ Все

☒ Только

Со сценариями JavaScript
С настроенными действиями при открытии (OpenActions)
С настроенными действиями (Actions) Со встроенными объектами
Зашифрованные Защищенные

Продолжительность наблюдения за файлом

2 минуты 0 секунд

По истечении этого времени анализ файла будет прерван с сохранением результатов

☒ Расшифровывать и анализировать HTTPS-трафик

☐ Отключить запись видео

[Объекты, подходящие под правило](#) 

Изменить

Отмена

Удалить

Рисунок 18. Выбор продолжительности наблюдения за файлом

Как результат, для проверок в поведенческом анализе на Windows получаем следующий набор правил.

☒ Поведенческий анализ

Вы можете указать параметры анализа и выбрать образ ВМ для различных типов файлов.

☒ Executables Windows								
Типы файлов	Образ виртуальной машины	Продолжительность наблюден...	Расшифровывать и анализиров...	Отключить запись видео				
Файлы приложений, Исполняе...	win10-1803-x64	4 мин	Да	Нет				

☒ Office files Windows								
Типы файлов	Метки	Образ виртуальной маши...	Продолжительность набл...	Расшифровывать и анали...	Отключить запись видео			
PUB, Документы, Презент...	С макросами Со встроенным	win10-1803-x64	3 мин	Да	Нет			

☒ PDF Windows								
Типы файлов	Метки	Образ виртуальной машины	Продолжительность наблюд...	Расшифровывать и анализир...	Отключить запись видео			
PDF	Содержит JavaScript Содержит C	win10-1803-x64	2 мин	Да	Нет			

Рисунок 19. Набор правил для проверок в поведенческом анализе

3.4. Создание правила для исполняемых файлов, Linux

В качестве второго примера набора правил рассмотрим настройку для семейства GNU/Linux, из которого выберем образ Ubuntu 22.04.5 LTS (Jammy Jellyfish) x64. Здесь обратим внимание, что в семействе GNU/Linux могут быть отличия типов анализируемых установочных пакетов в зависимости от базы дистрибутива (RPM или Debian).

Первым настроим правило проверки на следующие **Типы проверяемых файлов**: исполняемые (приложения и системные) файлы.

Добавление правила



Название

Executables Ubuntu

Образ виртуальной машины

ubuntu-jammy-x64 (Ubuntu 22.04.5 LTS (Jammy Jellyfish) x64)

Файлы будут проверяться в виртуальной машине, развернутой из этих образов

Типы проверяемых файлов

Исполняемые файлы ✕

Исполняемые файлы

- Установочные пакеты
 - DEB
- Для семейства Linux
 - ELF
 - SH
- Java
- Мультиплатформенные скрипты

Рисунок 20. Создание правила для исполняемых файлов, Linux

Продолжительность наблюдения за файлом — 4 минуты.

Добавление правила



Название

Executables Ubuntu

Образ виртуальной машины

ubuntu-jammy-x64 (Ubuntu 22.04.5 LTS (Jammy Jellyfish) x64)

Файлы будут проверяться в виртуальной машине, развернутой из этих образов

Типы проверяемых файлов

Исполняемые файлы ×



Чем больше типов, тем больше может быть очередь файлов на проверку

Продолжительность наблюдения за файлом

4

минуты

0

секунд

По истечении этого времени анализ файла будет прерван с сохранением результатов

☒ Расшифровывать и анализировать HTTPS-трафик

☐ Отключить запись видео

[Объекты, подходящие под правило](#)

Рисунок 21. Выбор продолжительности наблюдения за файлом

3.5. Создание правила для офисных приложений, Linux

Вторым настроим правило для файлов офисных приложений.

Добавление правила

x

Название

Office files Ubuntu

Образ виртуальной машины

ubuntu-jammy-x64 (Ubuntu 22.04.5 LTS (Jammy Jellyfish) x64)

Файлы будут проверяться в виртуальной машине, развернутой из этих образов

Типы проверяемых файлов

Документы x Презентации x Таблицы x

🔍 |

▼ ☒ Все

> ☐ Исполняемые файлы ⚠️

▼ ☒ Файлы офисных приложений

> ☒ Документы

> ☒ Презентации

> ☒ Таблицы

☐ PDF

Продолжительность наблюдения за файлом

2

минуты

0

секунд

По истечении этого времени анализ файла будет продолжен с помощью правил

Рисунок 22. Создание правила для офисных приложений, Linux

Для этих файлов обратим внимание на определенные песочницей **Метки**.

Добавление правила

x

Название

Office files Ubuntu

Образ виртуальной машины

☐ Зашифрованные

☒ С макросами

☒ Со встроенными объектами

☒ С элементами ActiveX

☒ С запросами к внешним данным

☒ Использующие шаблон

☒ С функциями DDE

☒ С настроенными действиями (Actions)

С макросами Со встроенными объектами С элементами ActiveX

С запросами к внешним данным Использующие шаблон

С функциями DDE С настроенными действиями (Actions)

С надстройками Office

Продолжительность наблюдения за файлом

2 минуты 0 секунд

По истечении этого времени анализ файла будет прерван с сохранением результатов

Добавить

Отмена

Рисунок 23. Добавление меток

Как правило, в поведенческом анализе есть смысл запускать файлы, метки в которых указывают на наличие активного содержимого. Это практически весь список, кроме метки **Зашифрованные**. Запуск файлов с такой меткой остается опциональным и зависит от политик ИБ в организации, но в общей практике его рекомендуется включить. **Продолжительность наблюдения за файлом**: если мы определяем проверку только объектов с метками (с точки зрения экономии ресурса поведенческого анализа) — выбираем 3 минуты.

Добавление правила



Файлы будут проверяться в виртуальной машине, развернутой из этих образов

Типы проверяемых файлов

Документы × Презентации × Таблицы × × ▾

Чем больше типов, тем больше может быть очередь файлов на проверку

Файлы офисных форматов

☐ Все

☒ Только

С макросами Со встроенными объектами С элементами ActiveX
С запросами к внешним данным Использующие шаблон
С функциями DDE С настроенными действиями (Actions)
С надстройками Office Зашифрованные ▾

Продолжительность наблюдения за файлом

минуты секунд

По истечении этого времени анализ файла будет прерван с сохранением результатов

☒ Расшифровывать и анализировать HTTPS-трафик

☐ Отключить запись видео

[Объекты, подходящие под правило](#)

Рисунок 24. Выбор продолжительности наблюдения за файлом

3.6. Создание правила для PDF-файлов, Linux

Третье правило — по оставшемуся типу PDF.

Добавление правила

✕

Название

PDF Ubuntu

Образ виртуальной машины

ubuntu-jammy-x64 (Ubuntu 22.04.5 LTS (Jammy Jellyfish) x64) ▾

Файлы будут проверяться в виртуальной машине, развернутой из этих образов

Типы проверяемых файлов

PDF ✕ ▾

Q

▾ Все

> ☐ Исполняемые файлы ⚠▾ ☒ Файлы офисных приложений> ☐ Документы ⚠> ☐ Презентации ⚠> ☐ Таблицы ⚠☒ PDF☒ Расшифровывать и анализировать HTTPS-трафик☐ Отключить запись видео

Добавить

Отмена

Рисунок 25. Создание правила для PDF-файлов, Linux

Для этих файлов обратим внимание на определенные песочницей **Метки**.

Добавление правила

x

ubuntu-jammy-x64 (Ubuntu 22.04.5 LTS (Jammy Jellyfish) x64) v

Файлы будут проверяться в виртуальной машине, развернутой из этих образов

Типы проверяемых файлов

PDF x

x

v

Чем больше типов, тем больше может быть очередь файлов на проверку

Файлы PDF

☐ Все

☒ Только

Со сценариями JavaScript

С настроенными действиями при открытии (OpenActions) v

С настроенными действиями (Actions)

Со встроенными объектами

☐ Зашифрованные

☒ Со сценариями JavaScript

☒ С настроенными действиями при открытии (OpenActions)

☒ С настроенными действиями (Actions)

☒ Со встроенными объектами

☐ Защищенные

Рисунок 26. Добавление меток

Отмечаем в раскрывающемся списке всё, кроме меток **Зашифрованные** и **Защищенные**. Запуск файлов с такими метками остается опциональным и зависит от политик ИБ в организации, но в общей практике его рекомендуется включить. Продолжительность: если мы определяем проверку только объектов с метками (с точки зрения экономии ресурса поведенческого анализа) — выбираем 2 минуты.

Добавление правила

✕

ubuntu-jammy-x64 (Ubuntu 22.04.5 LTS (Jammy Jellyfish) x64) ▾

Файлы будут проверяться в виртуальной машине, развернутой из этих образов

Типы проверяемых файлов

PDF ✕ ▾

Чем больше типов, тем больше может быть очередь файлов на проверку

Файлы PDF

☐ Все

☒ Только

Со сценариями JavaScript

С настроенными действиями при открытии (OpenActions) ▾

С настроенными действиями (Actions)

Со встроенными объектами

Зашифрованные

Защищенные

Продолжительность наблюдения за файлом

2

минуты

0

секунд

По истечении этого времени анализ файла будет прерван с сохранением результатов

Добавить

Отмена

Рисунок 27. Выбор продолжительности наблюдения за файлом

Как результат, для проверок в поведенческом анализе на Ubuntu 22.04 LTS (Jammy Jellyfish) x64 получаем следующий набор правил.

Executables Ubuntu									
Типы файлов	Образ виртуальной машины		Продолжительность наблюдения з...	Расшифровывать и анализировать ...	Отключить запись видео				
Исполняемые файлы	ubuntu-jammy-x64		4 мин	Да	Нет				

Office files Ubuntu									
Типы файлов	Метки	Образ виртуальной маши...		Продолжительность набл...	Расшифровывать и анали...	Отключить запись видео			
Документы, Презентации,...	С макросами	Со встроенным	ubuntu-jammy-x64	3 мин	Да	Нет			

PDF Ubuntu									
Типы файлов	Метки	Образ виртуальной машины		Продолжительность набл...	Расшифровывать и анализир...	Отключить запись видео			
PDF	Содержит JavaScript	Содержит C	ubuntu-jammy-x64	2 мин	Да	Нет			

Рисунок 28. Набор правил для проверок в поведенческом анализе

После создания правил примените изменения в источнике, нажав кнопку **Сохранить**.

Для полноты проверок в инфраструктурах, где используются оба семейства ОС, основная практика — проверка файлов в обоих семействах. Если же стоит вопрос экономии ресурса, то допустимо снять дублирующие проверки одних и тех же типов файлов на разных видах образов.

4. Проверка правил

После сохранения параметров проверки для источника рекомендуется проследить за результатами проверки на потоке проверяемых файлов, в том числе возможно использование сервисов проверки защищенности. При обнаружении в результате проверок некорректных срабатываний (ложноположительных или ложноотрицательных) необходимо перенастроить наборы правил.



Positive Technologies — лидер в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 4000 организаций по всему миру. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 205 тысяч акционеров.