Kaspersky Security Center 10 SP3  
Kaspersky Endpoint Security 11

Пилотное тестирование

**Исключения из проверки**

В этих сценариях вы проверите новые возможности исключить файл или папку из проверки.

## Расскажите о себе:

|  |  |
| --- | --- |
| Полное имя |  |
| Компания |  |
| E-mail |  |
| Телефон |  |

## Подготовьте:



* На один компьютер (Сервер администрирования) установите Kaspersky Security Center 10 SP3
* На другой компьютер (клиентский компьютер) установите Kaspersky Endpoint Security 11 и Агент администрирования
* Подключите Агент администрирования на клиентском компьютере к Серверу администрирования
* Создайте три тестовых вредоносных файла с разными контрольными суммами, например:
  + FalsePositive1.com — файл с оригинальной строкой EICAR-TEST-VIRUS
  + FalsePositive2.com — файл с оригинальной строкой EICAR-TEST-VIRUS и пробелом в конце
  + FalsePositive3.com — файл с оригинальной строкой EICAR-TEST-VIRUS и символом перевода строки в конце (или двумя пробелами)
* Поместите FalsePositive3.com в ZIP-архив: FalsePositive3.zip

|  |  |  |
| --- | --- | --- |
|  | Сервер администрирования | Клиентский компьютер |
| Операционная система |  |  |
| Версия Kaspersky Security Center |  |  |
| Версия Kaspersky Endpoint Security |  |  |

# Сценарий 1. Исключите файл по контрольной сумме, посчитанной из образца файла

На Сервере администрирования

1. Запустите Консоль администрирования Kaspersky Security Center
2. Перейдите в узел Policies и откройте политику Kaspersky Endpoint Security 11 for Windows
3. В политике перейдите в раздел General settings | Exclusions
4. Нажмите кнопку Settings в секции Scan exclusions and trusted zone
5. Добавьте исключение, нажмите кнопку Add над списком исключений
6. Отметьте параметр Hash в области Properties
7. Кликните по ссылке enter object hash… в области Scan exclusion description
8. В окне Hash нажмите кнопку Browse и выберите Select file
9. В окне Open укажите файл FalsePositive1.com и нажмите Open

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| В окне Hash отображается последовательность символов, похожая на Hash-сумму файла |  |

1. Закройте окно Hash: нажмите OK
2. Закройте окно Scan exclusion: нажмите OK

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Внизу списка исключений появилось новое исключение, отмеченное галкой и с заполненным полем Hash |  |

1. Закройте окно Trusted zone: нажмите OK
2. Подтвердите изменение политики: нажмите Yes. Подтверждение нужно, если индикатор безопасности политики не “зеленый”.
3. Сохраните политику: нажмите OK
4. Подождите пока политика применится к компьютерам и еще секунд 30

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Политика применилась к компьютерам |  |

На клиентском компьютере

1. Скопируйте на рабочий стол файлы FalsePositive1.com, FalsePositive2.com и FalsePositive3.zip

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Файл FalsePositive2.com не скопиров |  |

1. Откройте окно Kaspersky Endpoint Security (кликните по иконке в панели уведомлений)
2. Нажмите кнопку Reports
3. Откройте отчет File Threat Protection

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
|  |  |
| информационное сообщение о файле FalsePositive1.com; серия критических и предупреждающих сообщений о файле FalsePositive2.com; никаких сообщений о файле FalsePositive3.zip |  |

# Сценарий 2. Исключите файл по контрольной сумме, взятой из события обнаружения

В консоли Kaspersky Endpoint Security на Сервере администрирования

1. Выберите узел Administration Server
2. Перейдите на закладку Events
3. Проверьте, что выбрана выборка Recent events и нажмите Run selection

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| В списке есть событие о том, что обнаружен вредоносный файл FalsePositive2.com |  |

1. Вернитесь в узел Policies и откройте политику Kaspersky Endpoint Security 11 for Windows
2. Перейдите в раздел General Settings | Exclusions
3. Нажмите кнопку Settings в секции Scan exclusions and trusted zone
4. Добавьте новое исключение, нажмите Add
5. В окне Scan exclusion отметьте параметр Hash в области Properties
6. Кликните по ссылке enter object hash… в области Scan exclusion description
7. В окне Hash нажмите Browse и выберите Select from event

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| В окне отображается список событий Malicious object detected с hash-суммами обнаруженных объектов |  |

1. Выберите событие с именем компьютера и временем обнаружения, которые соответствуют файлу FalsePositive2.com и нажмите OK
2. В окне Hash нажмите OK
3. В окне Scan exclusion нажмите OK

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Внизу списка появилось еще одно исключения, отмеченное галкой, и с заполненным полем Hash |  |

1. Закройте окно Trusted zone: нажмите OK
2. Сохраните политику: нажмите OK
3. Подождите пока политика применится к компьютерам и еще 30 секунд

На клиентском компьютере

1. Еще раз скопируйте на рабочий стол файл FalsePositive2.com

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Файл успешно скопировался |  |

# Сценарий 3. Создайте исключение со спецсимволом \*\*

В консоли KSC на Сервере администрирования

1. Выберите узел Policies и откройте политику Kaspersky Endpoint Security 11 for Windows
2. Перейдите в раздел General Settings | Exclusions
3. Добавьте исключение: нажмите Add
4. В окне Scan exclusion отметьте параметр File or folder в области Properties
5. Кликните по ссылке select file or folder… в области Scan exclusion description
6. В окне Name of file or folder введите %SystemDrive%\Users\\*\AppData\Local\\*\*\FalsePositive\*.\* и нажмите OK
7. Закройте окно Scan Exclusion: нажмите OK

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Внизу списка исключений есть исключение, отмеченное галкой, и с заполненным полем File or folder |  |

1. Закройте окно Trusted zone: нажмите OK
2. Подтвердите изменения, нажмите Yes
3. Закройте политику: нажмите OK
4. Подождите, пока политика применится к клиентским компьютерам и еще 30 секунд

На клиентском компьютере

1. Откройте папку %Temp% в проводнике Windows
2. Ожидаемый результат: открылась папка C:\Users\<имя пользователя>\AppData\Local\Temp
3. Отройте архив FalsePositive3.zip и скопируйте из него файл FalsePositive3.com в папку %temp%

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Файл FalsePositive3.com успешно скопировался |  |

1. В проводнике Windows перейдите в папку C:\Users\<имя пользователя>\AppData\Local\
2. Создайте новую папку MyApp
3. Скопируйте в нее файл FalsePositive3.com

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Файл FalsePositive3.com успешно скопировался |  |

1. Скопируйте файл FalsePositive3.com на рабочий стол

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Файл пропал с рабочего стола спустя 5–10 секунд |  |

1. Откройте окно Kaspersky Endpoint Security 11 (кликните по иконке в панели уведомления)
2. Нажмите кнопку Reports
3. Выберите отчет File Threat Protection

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| В журнале есть критическое событие о том, что в файле FalsePositive3.com на рабочем столе обнаружена угроза, событий об этом файле в папке %Temp% и в папке MyApp нет |  |

### Комментарии

|  |
| --- |
|  |