Kaspersky Security Center 10 SP3  
Kaspersky Endpoint Security 11

Пилотное тестирование

**Вердикты расширенной защиты**

В этих сценариях вы проверите, как Kaspersky Endpoint Security реагирует на опасное поведение файлов и попытки эксплойтов.

## 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, можно Windows Server) установите Kaspersky Endpoint Security 11 и Агент администрирования
* Подключите Агент администрирования на клиентском компьютере к Серверу администрирования
* Подготовьте тестовый файл Meicar.exe
* Создайте три тестовых вредоносных bat-файла:
  + behavior1.bat:  
    echo test > C:\TestBssDetectAction.tst
  + behavior2.bat:  
    copy Meicar.exe > C:\TestBssDetectAction.tst
  + exploit.bat:  
    echo test > C:\TestBssBlockingDetectAction.tst

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

# Сценарий 1. Проверьте, как Kaspersky Endpoint Security обнаруживает вредоносные программы по поведению

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 Essential Threat Protection | File Threat Protection
4. Выключите защиту файлов: снимите отметку напротив имени компонента File Threat Protection
5. Точно так же выключите остальные компоненты в разделе Essential Threat Protection: Web Threat Protection, Mail Threat Protection, Firewall, Network Threat Protection и BadUSB Attack Prevention
6. Перейдите в раздел Advanced Threat Protection | Host Intrusion Prevention
7. Отключите компонент: снимите отметку возле имени компонента Host Intrusion Prevention
8. Перейдиете в раздел Advanced Threat Detection | Behavior Detection
9. Проверьте, что компонент включен, а если нет, включите его: установите отметку возле имени компонента Behavior Detection
10. Сохраните политику: нажмите OK

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Kaspersky Security Center просит подтвердить, что вы хотите снизить уровень безопасности |  |

1. Подтвердите снижение уровня безопасности: нажмите Yes
2. Подождите, пока политика применится к компьютерам и еще 30 секунд

На клиентском компьютере

1. Откройте в проводнике Windows корень диска C:
2. Проверьте, что там нет файла с именем TestBssDetectAction.tst
3. Скопируйте на рабочий стол файл behavior1.bat
4. Выполните behavior1.bat с правами администратора
5. Откройте интерфейс Kaspersky Endpoint Security
6. Откройте отчеты: нажмите кнопку Reports
7. Откройте журнал Behavior Detection

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| В журнале 3 события о файле behavior1.bat: Malicious object detected, A backup copy of the object was created и Object deleted; файла behavior1.bat на рабочем столе больше нет |  |

1. Закройте окна Kaspersky Endpoint Security
2. Удалите файл TestBssDetectAction.tst из корня диска C:

# Сценарий 2. Проверьте, как Kaspersky Endpoint Security откатывает действия опасной программы

В консоли Kaspersky Endpoint Security на Сервере администрирования

1. Перейдите в узел Policies и откройте политику Kaspersky Endpoint Security 11 for Windows
2. Host Intrusion Prevention
3. Перейдиете в раздел Advanced Threat Detection | Remediation Engine
4. Проверьте, что компонент включен, а если нет, включите его: установите отметку возле имени компонента Remediation Engine
5. Сохраните политику: нажмите OK

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Kaspersky Security Center просит подтвердить, что вы хотите применить политику с низким уровнем безопасности |  |

1. Подтвердите, что хотите применить политику: нажмите Yes
2. Подождите, пока политика применится к компьютерам и еще 30 секунд

На клиентском компьютере

1. Откройте в проводнике Windows корень диска C:
2. Проверьте, что там нет файла с именем TestBssDetectAction.tst
3. Скопируйте на рабочий стол файлы Meicar.exe и behavior2.bat
4. Выполните behavior2.bat с правами администратора
5. Откройте интерфейс Kaspersky Endpoint Security
6. Откройте отчеты: нажмите кнопку Reports
7. Откройте журнал Behavior Detection

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| В журнале 5 события о файле behavior2.bat: Malicious object detected, A backup copy of the object was created, Object deleted, Object deleted и Rollback completed; файла behavior2.bat на рабочем столе больше нет |  |

1. Закройте окна Kaspersky Endpoint Security
2. Откройте в проводнике Windows корень диска C:

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| На диске C: нет файла TestBssDetectAction.tst |  |

# Сценарий 3. Проверьте, как Kaspersky Endpoint Security блокирует эксплойты

В консоли Kaspersky Security Center на Сервере администрирования

1. Перейдите в узел Policies и откройте политику Kaspersky Endpoint Security 11 for Windows
2. Перейдиете в раздел Advanced Threat Detection | Exploit Prevention
3. Проверьте, что компонент включен, а если нет, включите его: установите отметку возле имени компонента Exploit Prevention
4. Сохраните политику: нажмите OK

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Kaspersky Security Center просит подтвердить, что вы хотите применить политику с низким уровнем безопасности |  |

1. Подтвердите, что хотите применить политику: нажмите Yes
2. Подождите, пока политика применится к компьютерам и еще 30 секунд

На клиентском компьютере

1. Откройте в проводнике Windows корень диска C:
2. Проверьте, что там нет файла с именем TestBssBlockingDetectAction.tst
3. Скопируйте на рабочий стол файл exploit.bat
4. Выполните exploit.bat с правами администратора
5. Откройте интерфейс Kaspersky Endpoint Security
6. Откройте отчеты: нажмите кнопку Reports
7. Откройте журнал Exploit Prevention

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| В журнале 2 события о файле exploit.bat: Malicious object detected и Blocked; файл exploit.bat остался на рабочем столе |  |

1. Закройте окна Kaspersky Endpoint Security
2. Удалите файл TestBssBlockingDetectAction.tst из корня диска C:

### Комментарии

|  |
| --- |
|  |