?????????? ??? KATA 7.* - ???????? ???? ??????????, ??? ??? ????????

IDS???????????? (SPAN)

Для проверки IDS-обнаружений (SPAN) можно использовать утилиту `tcpreplay` на сервере, сконфигурированном для получения трафика SPAN.

Пакет `tcpreplay` не устанавливается по умолчанию, поэтому его нужно установить вручную. Следуйте инструкции ниже:

1. Скачайте пакет `tcpreplay_4.3.2-1build1_amd64.deb` по ссылке.
2. Скопируйте загруженный файл на узел KATA, например с помощью `scp`:

   ```
   [user@host]$ scp <your-path>/tcpreplay_4.3.2-1build1_amd64.deb admin@<kata-ip>:/tmp
   ```

3. Установите пакет на узле KATA командой:

   ```
   [admin@katahost]$ sudo dpkg -i /tmp/tcpreplay_4.3.2-1build1_amd64.deb
   ```

После установки вы сможете использовать `tcpreplay` на KATA.

???????? ??????? EICAR

Загрузите пример EICAR-Test-File_TCP.pcap на сервер с SPAN-интерфейсом, затем выполните команду от имени `root`:

```
tcpreplay -i ens34 EICAR-Test-File_TCP.pcap    # ens34 в этом примере — SPAN-интерфейс
```

???????? ??????? Nmap

Сценарий такой же, как для Eicar, только используется другой файл `.pcap` (HackTool.Nmap.HTTP.C&C.pcap).

После тестирования детектов по SPAN рекомендуем отключить tx-capture обратно тем же способом, что и при включении.

AM Engine

Для проверки антивирусного (AM) движка используйте тестовый файл EICAR (www.eicar.com).

- **Почта:** отправьте файл EICAR по SMTP на порт 25 узла KATA (обработка SMTP должна быть включена). Для простоты можно воспользоваться локальным клиентом `swaks` на узле Central Node, чтобы не настраивать почтовую систему.

Пример использования `swaks`:

```
swaks --server 127.0.0.1 --port 25 --from antony@test.org --to cleopatra@test.org --attach eicar.com
swaks --server 127.0.0.1 --port 25 --from antony@test.org --to cleopatra@test.org --body "link_to_EICAR_here"
```

- **Конечная точка:** поместите файл EICAR на рабочую станцию и отправьте его в очередь на проверку при помощи задания GetFile.

?????????? YARA

По умолчанию в продукте нет правил YARA. Для тестирования можно использовать тестовое правило из документации YARA (writingrules):

```
rule ExampleRule
{
    strings:
        $my_text_string = "text here"
        $my_hex_string  = { E2 34 A1 C8 23 FB }
    condition:
        $my_text_string or $my_hex_string
}
```

Это правило отметит любой анализируемый объект, содержащий строки `$my_text_string` или `$my_hex_string`.

?????????? TAA (IoA)

Проверка детектов IoA возможна только при наличии лицензии KEDR.

- Скопируйте файл `.bat` из прикреплённого архива Test_IOA.rar (пароль not_infected) в любую папку на хосте с установленным EDR и запустите его. Через несколько минут (KATA требуется время на передачу и обработку телеметрии) проверьте оповещения в KATA. В алерте должен быть тип `ioa_test_detect`. Если тестировать IoA на этом хосте повторно, файл `.bat` необходимо размещать в разные папки.
- На хосте с установленным KEA выполните в `cmd.exe` команду:

  ```
  wmic.exe "sfdgcall uninstallkasperskyblabla"
  ```

  Команда завершится ошибкой, но это не важно. Через несколько минут в веб-интерфейсе KATA появится новое IoA-срабатывание.

?????????? TAA ?? ??????? ???????

Чтобы проверить TAA-срабатывания по цепочке событий, сначала убедитесь, что эта функция включена в веб-интерфейсе KATA (и что ресурсы заказчика позволяют её включить).

Затем на одной из подключённых машин EDR распакуйте архивы и запустите сценарии `.bat`:

- short_term_user_creation_complex.7z
- multiple_login_attempts_with_the_same_account_complex.7z

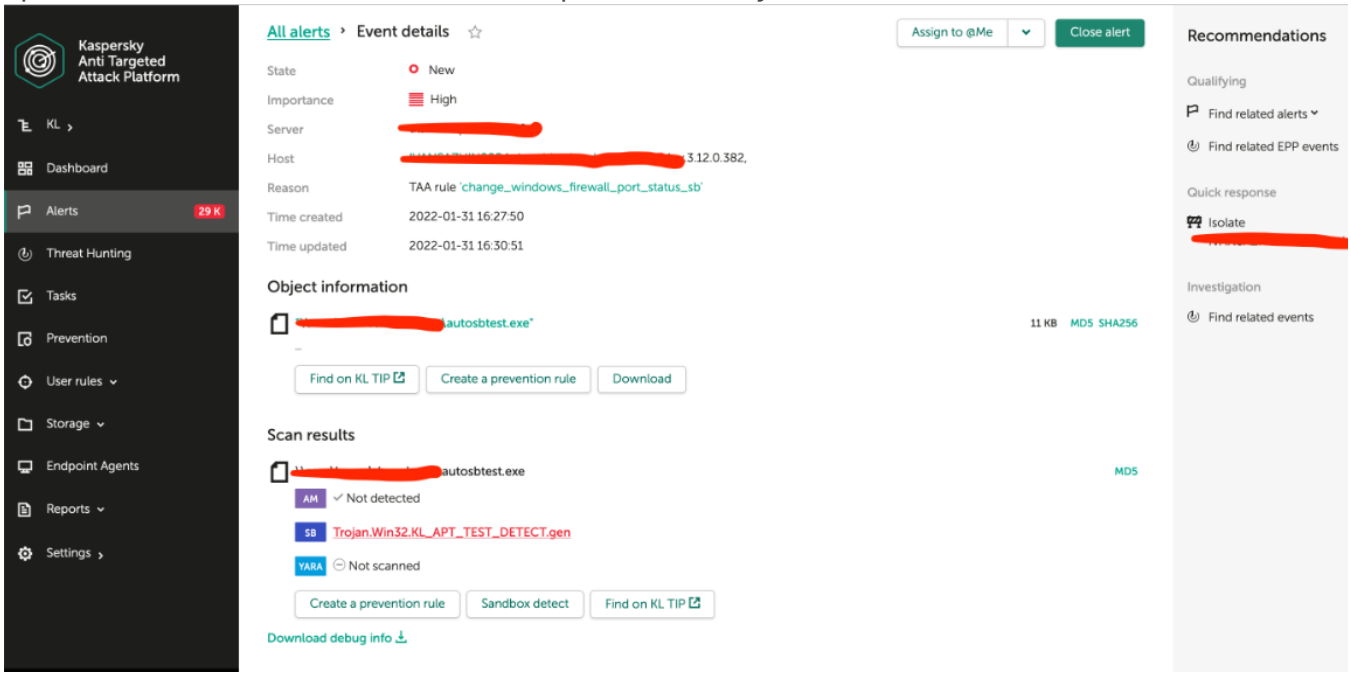
?????????? IoC

Для тестирования можно использовать собственное правило: архив loctest.zip (пароль *infected123*) срабатывает на запуск `c:\windows\system32\calc.exe`.

????????????? ????????? ? EDR

Для проверки автоматической песочницы:

- Распакуйте архив с образцом и используйте пароль для образцов по умолчанию: autosbtest.zip.
- **Важно:** не меняйте MD5-хэш образца.
- Запустите образец на защищённом EDR хосте и дождитесь автоматического срабатывания песочницы (verdict *Suspicious Activity*).



Для KESL: используйте файлы из архива, чтобы вызвать срабатывание песочницы и KESL:

- Распакуйте архив test_ioa_sb_linux.7z (пароль «infected») и скопируйте скрипт `test_ioa_sb_linux.sh` вместе с файлом `kl_kata_demo_starter` на хост с KESL (например, через WinSCP).
- Проверьте разрешения на файлы: если они не исполняемые, выполните команду:

```
sudo chmod 777 <файл>
```

- Запустите скрипт командой `./test_ioa_sb_linux.sh` и дождитесь появления алерта в KATA.

???????? ????????? (Sandbox detect)

Для проверки песочницы можно использовать файл `SA_sleep.exe` из архива no_am_detection sample.rar. Пароль хранится в текстовом документе внутри архива.

1. Перейдите в веб-интерфейс старшего офицера безопасности KATA.
2. Выберите меню **Хранилище → Загрузить** и загрузите файл `SA_sleep.exe` из архива для проверки KATA.

3. KATA поместит его в песочницу, и чуть позже SB должен вынести вердикт **Подозрительная активность**.
4. Если для `SA_sleep.exe` выдается вердикт «Not detected», используйте сценарий `test_sb.bat` из архива test_sb.zip.

???????? ????????? URL

Сначала убедитесь, что K(P)SN настроен и работает корректно. В этом примере хэш MD5 должен возвращать статус *UnTrusted*. Для проверки используйте команды:

```
Для KATA 4.+ и 5.0:
docker exec -it $(docker ps | grep ksn_proxy | awk '{print $1}') /opt/kaspersky/apt-ksn_proxy/sbin/ksn_client --ip 127.0.0.1 --hash 9C642C5B111EE85A6BCCFFC7AF896A51

Для KATA 5.1:
docker exec -it $(docker ps | grep ksn_proxy | awk '{print $1}') /opt/kaspersky/apt-ksn-proxy/sbin/ksn_client --ip 127.0.0.1 --hash 9C642C5B111EE85A6BCCFFC7AF896A51
```

Затем:

- **Трафик:** перейдите по адресу http://bug.qainfo.ru/TesT/Aphish_w/index.
- **Почта** (SMTP-обработка должна быть включена): отправьте ссылку из примера по электронной почте. Быстрый тест можно сделать с помощью команды `swaks`:

```
swaks --server 127.0.0.1 --port 25 --from fisherman@test.org --to cleopatra@test.org --body "http://bug.qainfo.ru/TesT/Aphish_w/index"
```

Revision #16
Created 21 August 2025 13:53:34 by Павел
Updated 6 February 2026 10:52:08 by Кирилл