Техническое ПМИ KATA 7.* - проверка всех технологий, что они работают

IDS-обнаружения (SPAN)

??? ???????? IDS???????????? (SPAN) ????? ???????????? ??????? `tcpreplay` ?? ???????, ????????????????? ??? ????????? ??????? SPAN.

????? `tcpreplay` ?? ?????????????? ?? ?????????, ??????? ??? ????? ?????????? ???????. ???????? ?????????? ????:

1. ???????? ????? `tcpreplay_4.3.2?1build1_amd64.deb` ?? ??????.
2. ?????????? ??????????? ???? ?? ???? KATA, ???????? ? ??????? `scp`:

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

3. ?????????? ????? ?? ???? KATA ????????:

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

????? ????????? ?? ??????? ???????????? `tcpreplay` ?? KATA.

Проверка трафика EICAR

????????? ?????? EICAR-Test-File_TCP.pcap ?? ?????? ? SPAN????????????, ????? ????????? ??????? ?? ????? `root`:

```
tcpreplay -i ens34 EICAR-Test-File_TCP.pcap    # ens34 ? ???? ??????? – SPAN??????????
```

Проверка трафика Nmap

???????? ????? ??, ??? ??? Eicar, ?????? ???????????? ?????? ???? `.pcap` (HackTool.Nmap.HTTP.C&C.pcap).

????? ???????????? ???????? ?? SPAN ?????????? ????????? tx?capture ??????? ??? ?? ????????, ??? ? ??? ?????????.

AM Engine

??? ???????? ????????????? (AM) ?????? ?????????? ???????? ???? EICAR (www.eicar.com).

- **Почта:** ????????? ???? EICAR ?? SMTP ?? ???? 25 ???? KATA (????????? SMTP ????? ???? ????????). ??? ???????? ????? ?????????????? ????????? ???????? `swaks` ?? ???? Central Node, ????? ?? ??????????? ???????? ???????.

?????? ????????????? `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:** ????????? ???? EICAR ?? ??????? ??????? ? ????????? ??? ? ??????? ?? ???????? ??? ?????? ??????? GetFile.

Обнаружения YARA

?? ????????? ? ???????? ??? ?????? YARA. ??? ??????????? ????? ??????????? ???????? ??????? ?? ???????????? 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
}
```

??? ??????? ??????? ????? ????????????? ??????, ?????????? ?????? `$my_text_string` ??? `$my_hex_string`.

Обнаружения TAA (IoA)

???????? ???????? IoA ???????? ?????? ??? ??????? ???????? KEDR.

- ?????????? ???? `.bat` ?? ????????????? ?????? Test_IOA.rar (?????? not_infected) ? ????? ????? ?? ????? ? ????????????? EDR ? ????????? ???. ????? ????????? ????? (KATA ????????? ????? ?? ???????? ? ????????? ??????????) ????????? ?????????? ? KATA. ? ?????? ?????? ???? ??? `ioa_test_detect`. ???? ??????????? IoA ?? ???? ????? ????????, ???? `.bat` ?????????? ????????? ? ?????? ?????.
- ?? ????? ? ????????????? KEA ????????? ? `cmd.exe` ???????:
  ```
  wmic.exe "sfdgcall uninstallkasperskyblabla"
  ```
  ??????? ?????????? ???????, ?? ??? ?? ?????. ????? ????????? ????? ? ????????????? KATA ???????? ????? IoA?????????????.

Обнаружения TAA по цепочке событий

????? ????????? TAA????????????? ?? ??????? ???????, ??????? ?????????, ??? ??? ??????? ???????? ? ????????????? KATA (? ??? ??????? ????????? ????????? ?? ????????).

????? ?? ????? ?? ???????????? ????? EDR ?????????? ?????? ? ????????? ???????? `.bat`:

- short_term_user_creation_complex.7z
- multiple_login_attempts_with_the_same_account_complex.7z

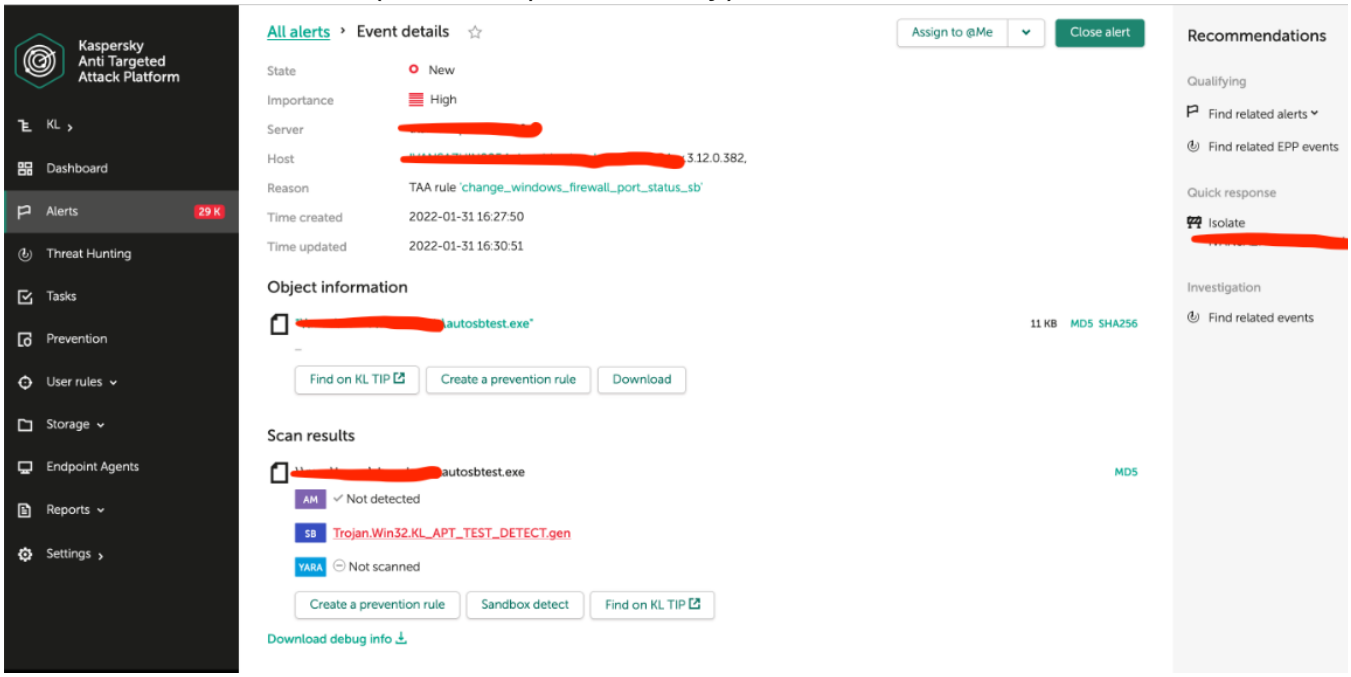
Обнаружения IoC

??? ???????????? ????? ???????????? ?????????? ???????: ????? Ioctest.zip (?????? *infected123*) ?????????? ?? ?????? `c:\windows\system32\calc.exe`.

Автоматическая песочница в EDR

??? ???????? ????????????? ?????????:

- ?????????? ????? ? ???????? ? ?????????? ?????? ??? ???????? ?? ?????????: autosbtest.zip.
- **Важно:** ?? ??????? MD5???? ???????.
- ????????? ??????? ?? ?????????? EDR ????? ? ????????? ????????????? ???????????? ????????? (verdict *Suspicious Activity*).



Для KESL: ?????????? ????? ?? ??????, ????? ??????? ???????????? ????????? ? KESL:

- ?????????? ????? test_ioa_sb_linux.7z (?????? «infected») ? ?????????? ?????? `test_ioa_sb_linux.sh` ?????? ? ?????? `kl_kata_demo_starter` ?? ???? ? KESL (????????, ????? WinSCP).
- ????????? ?????????? ?? ?????: ???? ??? ?? ???????????, ????????? ???????:

  ```
  sudo chmod 777 <????>
  ```

- ????????? ?????? ???????? `./test_ioa_sb_linux.sh` ? ????????? ????????? ?????? ? KATA.

Проверка песочницы (Sandbox detect)

??? ???????? ????????? ????? ???????????? ???? `SA_sleep.exe` ?? ?????? no_am_detection sample.rar. ?????? ???????? ? ????????? ????????? ?????? ??????.

1. ????????? ? ????????????? ???????? ??????? ???????????? KATA.
2. ???????? ???? **Хранилище → Загрузить** ? ????????? ???? `SA_sleep.exe` ?? ?????? ??? ????????? KATA.
3. KATA ???????? ??? ? ?????????, ? ???? ????? SB ?????? ??????? ??????? **Подозрительная активность**.
4. ???? ??? `SA_sleep.exe` ???????? ??????? «Not detected», ?????????? ???????? `test_sb.bat` ?? ?????? test_sb.zip.

Проверка репутации URL

??????? ?????????, ??? K(P)SN ???????? ? ???????? ?????????. ? ???? ??????? ??? MD5 ?????? ?????????? ?????? *UnTrusted*. ??? ???????? ??????????? ???????:

```
??? KATA 4.+ ? 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

??? 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
```

?????:

- **Трафик:** ????????? ?? ?????? http://bug.qainfo.ru/TesT/Aphish_w/index.
- **Почта** (SMTP?????????? ?????? ???? ????????): ????????? ?????? ?? ??????? ?? ??????????? ?????. ??????? ???? ????? ??????? ? ??????? ??????? `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 ?????
Updated 6 February 2026 10:52:08 by ??????