Проблемы ICAP интеграции

Troubleshooting ICAP интеграции KATA с внешними системами.

???? ????? ????????? ??? ???????????? ??? ?????????? ? ????????, ????????? ????????? ????????:

Проверка сетевой взаимосвязанности

1. ????????? ?????????? ????? CN/Sensor ? Proxy ?? ????? 1344 ? ??????? `tcpdump`:

```
tcpdump -i  port 1344 -nn
```

???????? ????????????? ???????????? ??????? tcpdump

???????? ???????????? ?????? (????????, ????????? ???? ????? ??????). ?????????, ??? tcpdump ????????? ?????? ??? ?????? ????? Proxy ? Sensor.

`???????? ?? ??????? ?entral Node`

Проверка со тсороны Central Node

`??????? ???????????? ??????`

Проверка со стороны Proxy

Сбор tcpdump для анализа трафика

1. ??? ???????? ?????????? ?? ????? 1344 ????? CN/Sensor ? ProxyServer ????????? ?? ?????? ?? ??????:

```
tcpdump -i  port 1344 -nn -w capture_filename.pcap
```

2. ??? ????? ? ??????? PCAP ?????? ????????????? ? ???????????? ???? Wireshark.
3. ??? ???????? ?????? ???????????? SCP/WinSCP, ????????:
4. ???????????? ? CN/Sensor ??? ProxyServer.
5. ????????? ? ???????, ??? ???????? tcpdump (????????, **/home/admin/**).
6. ???????? ???? ?? ????????? ?????????.

> **Примечание:** ?????? ?? ???????? ????????????? ??????????? ??????? **tcpdump**.

Проверка логов системы

1. ???????????? ? CN/Sensor ????? SSH ? ????????? ? Technical Support Mode.
2. ??? ???????? ????? ?????????:

```
sudo su
kata-collect-siem-logs log-history --output-dir /tmp --no-compress
kata-collect-siem-logs log-detects --output-dir /tmp --no-compress
```

??????? ???????????? ??????

В данный журнал пишутся файлы создавшие сработку в решении KATA

- ? `log-history.log` ?????????? ?????? ??? ???? ?????????? ??????.
- ? `log-detects.log` — ?????????? ?? ????????, ????????? ????????????.

3. ???????? ??????? ? ??????? SCP/WinSCP ?? ???????? **/tmp**.
4. ? ?????? ????? ??????? ?????? ?? ????????? ????? `ICAP`, ????? ????????? ? ????????? ? ??????? ??????? ?? ICAP-???????.

Просмотр логов сработки

??? ????????? ????? ?????? ICAP ?? ??????? CN/Sensor ???????????? ????? SSH ? ?????????:

```
sudo su
cat /var/log/kaspersky/services/preprocessor_icap/preprocessor_icap.log
```

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

- **стандартный режим:**

```
grep --color 'blocking_simple mode'
/var/log/kaspersky/services/preprocessor_icap/preprocessor_icap.log | grep 'verdict'
```

- **расширенный режим:**

```
grep --color 'blocking_advanced mode'
/var/log/kaspersky/services/preprocessor_icap/preprocessor_icap.log | grep 'verdict'
```

??????? ???????????? ??????

Советы по созданию заявки в службу технической поддержки

????? ???????? ??????? ????????? ??????? ? ????????? ????? ????????? ??????, ?????????????:

- ???????? ??? ????? ?????? ?????????? ?? ????????? KATA ? KEDR:
  - ?????? ? ????????????? ????????????,
  - ??????? ???????,
  - ???? ??????????,
  - ?????? ???????????? ???????????,
  - ???? ????????????? ????????.
- ??????????? ????????? ?????????? ????:
  - ?????? ???????,
  - tcpdump ? ????? ?????? (ICAP-?????? ? ICAP-??????),

    ```
    ??????: tcpdump -i ens192 port 1344 -nn -w capture_filename
    ```

- collect log ? CN/Sensor.
  ????? ?????? KDS

????? ??????? ???? ????????, ??? ????? ???????? ??? ?????????, ? ???? ??? ??????????????.

Revision #25
Created 30 June 2025 16:59:08 by ???????
Updated 6 February 2026 10:52:54 by ??????