???????? ICAP ??????????

Troubleshooting ICAP ?????????? KATA ? ???????? ?????????.

Если после настройки нет срабатываний или активности в графиках, выполните следующие действия:

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

1. Проверьте соединение между CN/Sensor и Proxy по порту 1344 с помощью `tcpdump`:

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

Описание функциональных возможностей команды **tcpdump**

Повторно сгенерируйте трафик (например, загрузите файл через прокси).
Убедитесь, что tcpdump фиксирует пакеты при обмене между Proxy и Sensor.

Проверка со тсороны Central Node

Проверка со тсороны Central Node

Процесс сканирования файлов

Проверка со стороны Proxy

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

1. Для проверки соединения по порту 1344 между CN/Sensor и ProxyServer выполните на каждой из сторон:

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

2. Эти файлы в формате PCAP удобно анализировать в инструментах типа Wireshark.
3. Для выгрузки файлов используйте SCP/WinSCP, например:
4. Подключитесь к CN/Sensor или ProxyServer.
5. Перейдите в каталог, где сохранен tcpdump (например, **/home/admin/**).
6. Скачайте файл на локальный компьютер.

> **Примечание:** Ссылка на описание функциональных возможностей команды **tcpdump**.

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

1. Подключитесь к CN/Sensor через SSH и перейдите в Technical Support Mode.
2. Для выгрузки логов выполните:

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

Процесс сканирования файлов

В данный журнал пишутся файлы создавшие сработку в решении KATA

- В `log-history.log` содержатся записи обо всех проверенных файлах.
- В `log-detects.log` — информация об объектах, вызвавших срабатывания.

3. Скачайте журналы с помощью SCP/WinSCP из каталога **/tmp**.
4. В файлах логов найдите записи по ключевому слову `ICAP`, чтобы убедиться в получении и анализе трафика от ICAP-клиента.

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

Для просмотра логов работы ICAP на стороне CN/Sensor подключитесь через SSH и выполните:

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

Для удобства анализа можно использовать фильтрацию по режимам сканирования:

- **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'
```

Процесс сканирования файлов

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

Чтобы ускорить решение возможных проблем и сократить время обработки заявки, рекомендуется:

- Соберите как можно больше информации об установке KATA и KEDR:
  - модель и характеристики оборудования,
  - уровень трафика,
  - типы интеграции,
  - версии программного обеспечения,
  - даты возникновения проблемы.
- Обязательно приложите актуальные логи:
  - журнал системы,
  - tcpdump с обеих сторон (ICAP-клиент и ICAP-сервер),

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

- collect log с CN/Sensor.
  Схема работы KDS

  - Четко опишите суть проблемы, при каких условиях она возникает, и шаги для воспроизведения.

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