KEDR 4.0-4.1

> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

> Официальная документация по данному разделу приведена в Онлайн-справке на продукт: https://support.kaspersky.com/help/KUMA/2.1/ru-RU/234627.htm

Настройка KEDR

Чтобы импортировать в KUMA события Kaspersky Endpoint Detection and Response 4.1, выполните следующие действия на стороне Kaspersky Endpoint Detection and Response:

1. Войдите в консоль управления того сервера Central Node, с которого вы хотите экспортировать события, по протоколу SSH или через терминал.

2. В ответ на приглашение системы введите имя учетной записи администратора и пароль, заданный при установке Kaspersky Endpoint Detection and Response.
Отобразится меню администратора компонента программы.

3. В меню администратора компонента программы выберите режим Technical Support Mode.

4. Нажмите на клавишу Enter.
Отобразится окно подтверждения входа в режим Technical Support Mode.

5. Подтвердите, что хотите выполнять действия с программой в режиме Technical Support Mode. Для этого выберите Yes и нажмите на клавишу Enter.

6. Выполните команду

```
sudo -i
```

7. В конфигурационном файле `/etc/sysconfig/apt-services` в поле `KAFKA_PORTS` удалите значение `10000`.

> Если к серверу Central Node подключены серверы Secondary Central Node или компонент Sensor, установленный на отдельном сервере, вам требуется разрешить соединение с сервером, на котором вы изменили конфигурационный файл, по порту

`10000`.

Настоятельно не рекомендуется использовать этот порт для каких-либо внешних подключений, кроме KUMA. Чтобы ограничить подключение по порту 10000 только для KUMA, выполните команду:

```
iptables -I INPUT -p tcp ! -s KUMA_IP_address --dport 10000 -j DROP
```

8. Выполните команду

```
systemctl restart apt_ipsec.service
```

9. В конфигурационном файле `/usr/bin/apt-start-sedr-iptables` в поле `WEB_PORTS` добавьте значение `10000` через запятую без пробела.

10. Выполните команду

```
sudo sh /usr/bin/apt-start-sedr-iptables
```

Настройка KUMA

1. На сервере KUMA добавьте IP-адрес сервера Central Node в формате `<IP-адрес> centralnode` в один из следующих файлов:

`%WINDIR%\System32\drivers\etc\hosts` – в случае сбора телеметрии KEDR агентом KUMA для Windows.

Как отредактировать файл hosts в Windows

1. Запустите cmd.exe от имени администратора

2. Выполните команду

```
notepad.exe %WINDIR%\System32\drivers\etc\hosts
```

3. Внести изменения в файл и сохраните (`Ctrl + S`)

`/etc/hosts` file – в случае сбора телеметрии KEDR коллектором или агентом KUMA для Linux.

2. В веб-интерфейсе KUMA создайте коннектор типа Kafka.
При создании коннектора укажите следующие параметры:

- В поле **URL** укажите **<IP-адрес сервера Central Node>:10000**
- В поле **Topic** укажите **EndpointEnrichedEventsTopic**.
- В поле **Consumer** group укажите любое уникальное имя.

3. В веб-интерфейсе KUMA создайте коллектор.

4. На шаге **Транспорт** укажите коннектор, созданный на шаге 2.

5. На шаге **Парсинг** событий выберите нормализатор **[OOTB] KEDR telemetry**.

6. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:

- Хранилище. Для отправки обработанных событий в хранилище.
- Коррелятор. Для отправки обработанных событий в коррелятор.
Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

7. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

8. Скопируйте появившуюся команду для установки коллектора KUMA.

Полезные ссылки

Настройка получения событий KATA/EDR (онлайн-справка KUMA):

https://support.kaspersky.com/help/KUMA/2.1/ru-RU/234627.htm

Revision #10
Created 11 August 2023 08:19:11 by Koala
Updated 7 July 2024 08:58:31 by Koala