KEDR 5.0-6.0

> 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

> При импорте событий из Kaspersky Endpoint Detection and Response 5.0 действует ряд ограничений:
> - Импорт событий доступен только для неотказоустойчивой версии Kaspersky Endpoint Detection and Response.
> - Импорт событий доступен, если в программе Kaspersky Endpoint Detection and Response используются лицензионные ключи KATA и KEDR.
> - Импорт событий не доступен, если в составе программы Kaspersky Endpoint Detection and Response используется компонент Sensor, установленный на отдельном сервере.

Чтобы импортировать в KUMA события Kaspersky Endpoint Detection and Response 5.0, 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 `/usr/local/lib/python3.8/dist-packages/firewall/create_iptables_rules.py` укажите дополнительный порт `10000` для константы `WEB_PORTS`:

```
WEB_PORTS = f'10000,80,{AppPort.APT_AGENT_PORT},{AppPort.APT_GUI_PORT}'
```

Для **KATA 6.0** файл находится по пути `/opt/venv/lib/python3.11/site-packages/firewall/create_iptables_rules.py` и строку надо отредактировать в таком виде:

```
WEB_PORTS = '10000,80,' + ','.join(
```

8. Выполните команды:

> Кластерная подсеть по умолчанию: 198.18.0.0/16

```
kata-firewall stop
kata-firewall start --cluster-subnet <маска сети для адресации серверов кластера>
```

Настройка KUMA

1. На сервере KUMA добавьте IP-адрес сервера Central Node в формате `<IP-адрес> kafka.services.external.dyn.kata` 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.

Случай с несколькими серверами KEDR

При наличии двух серверов EDR брокер на обоих узлах в метаданных передает одно и то же имя centralnode. Таким образом, выгрузка телеметрии через Кафку одновременно с двух разных узлов EDR становится невозможной, так как они просят клиента обращаться по одному и тому же некорректному адресу http://centralnode:10000.

Для решения проблемы:

1. на одной CN выгрузим параметры, с которым контейнер стартует:

```
console-settings-updater get /kata/configuration/product/kafka | python3 -m json.tool > /tmp/kafka.conf
```

2. Откроем в редакторе файл: `vim kafka.conf` и исправляем строку `"external_address": "kafka.services.external.dyn.kata"` на `"external_address": "kafka2.services.external.dyn.kata"`

3. Загружаем файл обратно в контейнер:

```
console-settings-updater set /kata/configuration/product/kafka @/tmp/kafka.conf
```

Revision #8
Created 11 August 2023 09:06:05 by Koala
Updated 25 December 2024 14:38:26 by Koala