KEDR 5.1-6.0 (Телеметрия EDR по API)

> Данная инструкция предназначена для версии KUMA 3.0.2, а также версий KATA 5.1 и 6.0

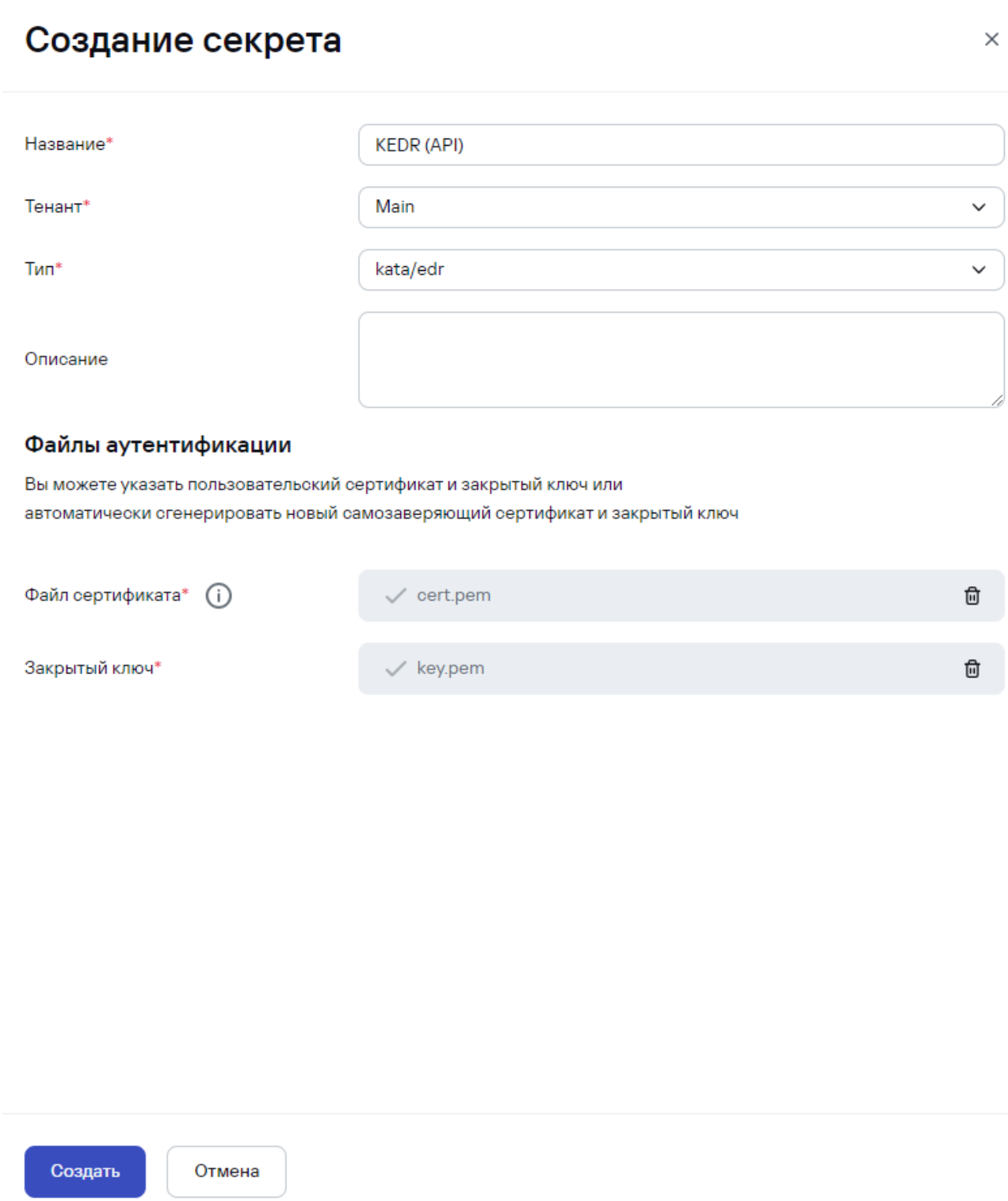
> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

> Официальная документация по данному разделу приведена в Онлайн-справке на продукт: https://support.kaspersky.com/help/KUMA/3.0.2/ru-RU/261000.htm

Создание секрета

Для подключения KEDR со стороны KUMA по API необходимо создать секрет для аутентификации. Для этого выполните следующие действия:

1. В веб-интерфейсе KUMA перейдите на вкладку **Ресурсы → Секреты** и нажмите на кнопку **Добавить**.
2. Укажите **Имя** секрета, выберите **Тенант**, к которому будет относиться создаваемый секрет.
3. Нажмите **Сгенерировать и скачать сертификат и закрытый ключ шифрования соединения**, после чего произойдет скачивание архива.
4. Распакуйте архив. Внутри будут файл сертификата и файл закрытого ключа.
5. Укажите **Файл сертификата** и **Закрытый ключ** в соответствии с рисунком:



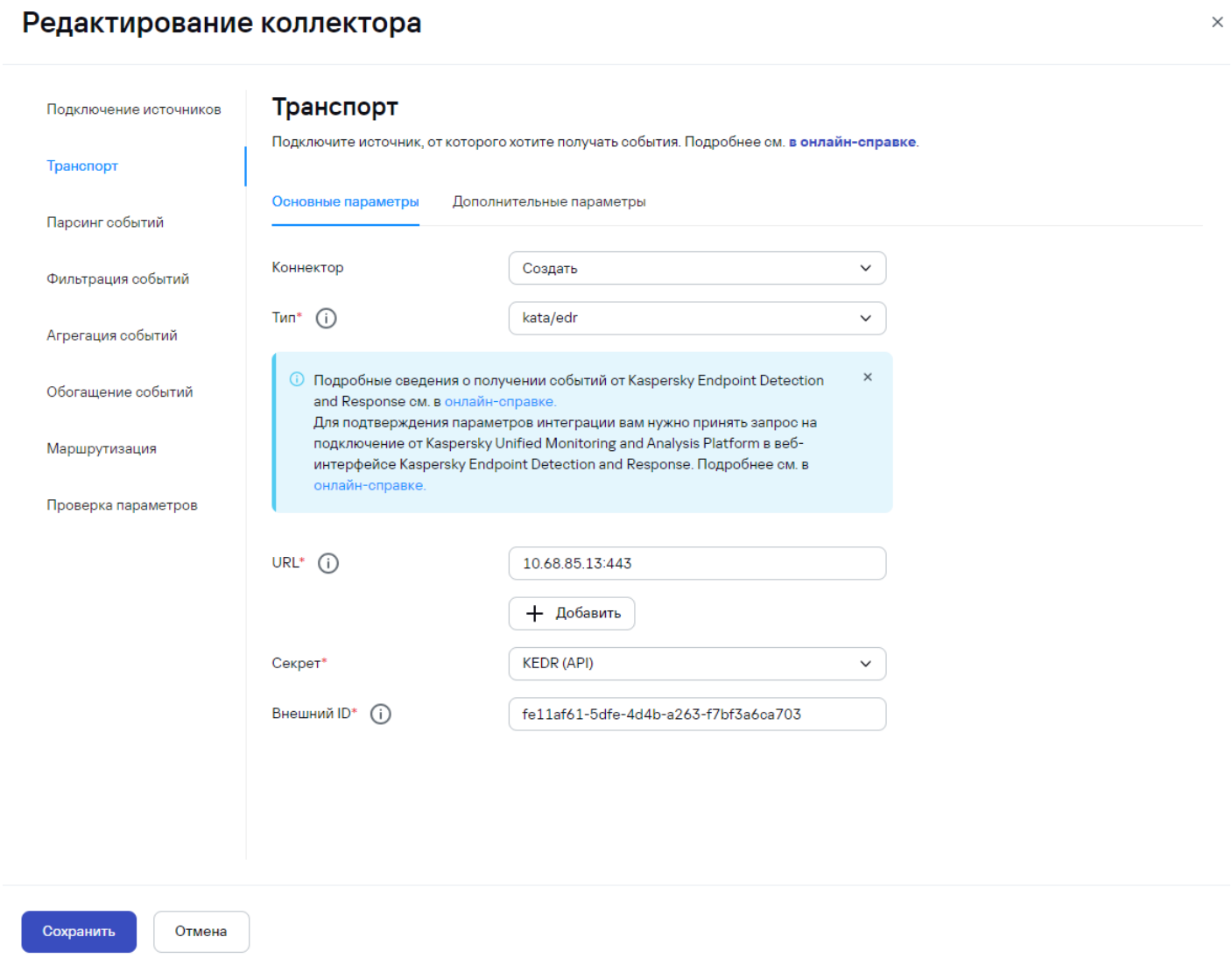
6. Сохраните секрет

Настройка коллектора

После того как был создан секрет, требуется создать коллектор в веб-интерфейсе KUMA для событий KEDR.

1. На шаге **Транспорт** укажите тип **kata/kedr** и **URL** в формате <IP-адрес или FQDN CN

KATA>:<порт, по умолчанию 443>), в поле **Секрет** укажите ранее созданный секрет.



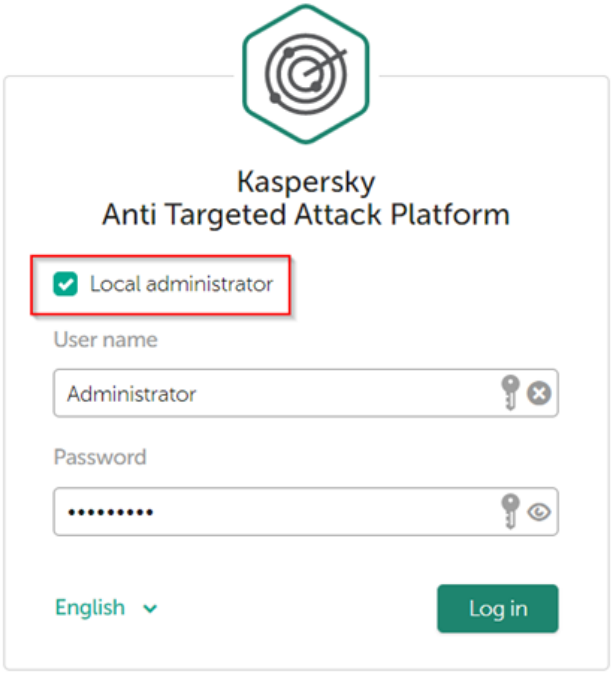
2. На шаге **Парсинг** событий выберите нормализатор **[OOTB] KEDR telemetry**.
3. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:
- **Хранилище**. Для отправки обработанных событий в хранилище.
- **Коррелятор**. Для отправки обработанных событий в коррелятор.
Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.
4. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.
5. Скопируйте появившуюся команду для установки коллектора KUMA.

> В **Дополнительных параметрах** транспорта параметр **Время ожидания получения событий** означает время, за которое KATA собирает события для отправки.

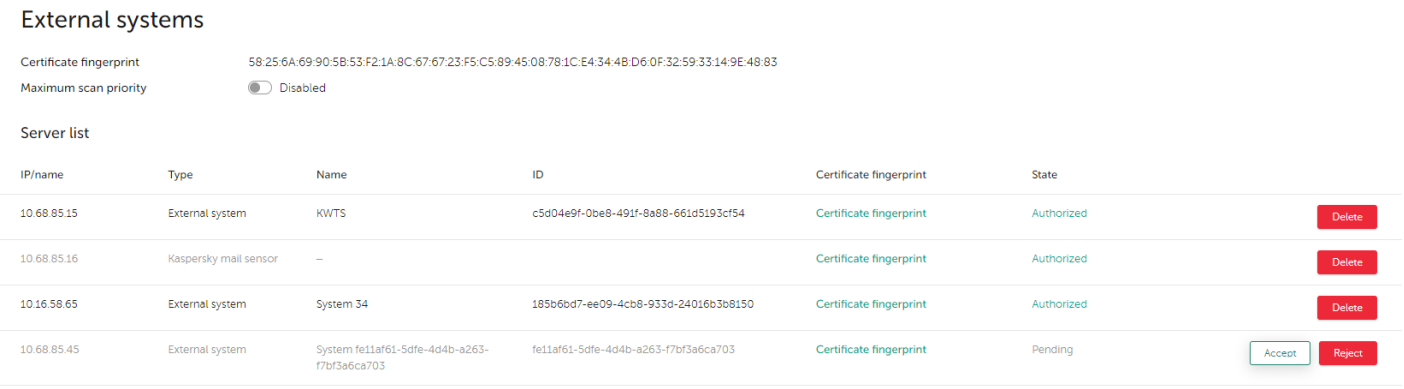
Настройка KATA

Для настройки сбора событий телеметрии из KATA в SIEM KUMA необходимо выполнить следующие действия:

1. Перейти в веб-консоль центрального узла Kaspersky Anti Targeted Attack из-под учетной записи Администратора, предварительно отметив параметр **Local administrator**



2. Перейти в раздел **External systems** и нажать **Accept** (для дальнейшего удобства вы можете изменить содержимое поля **Name,** например, на KUMA). Также следует проверить, что значение в поле **ID** совпадает со значением поля **Внешний ID** в настройках транспорта коллектора KUMA.



Полезные ссылки

Подробные сведения о получении событий от Kaspersky Endpoint Detection and Response: https://support.kaspersky.com/KATA/5.1/ru-RU/248949.htm

Импорт событий Kaspersky Endpoint Detection and Response с помощью коннектора kata/edr: https://support.kaspersky.com/help/KUMA/3.0.2/ru-RU/261000.htm

---

Revision #8
Created 22 January 2024 08:15:26 by lithium
Updated 7 July 2024 08:58:58 by Koala