

KEDR 5.1-6.0 (Телеметрия EDR по API)

✓ **Рекомендуется** - Рекомендуемый способ сбора для этого источника событий

Данная инструкция предназначена для версии KUMA с 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:




Создание секрета



Название*	<input type="text" value="KEDR (API)"/>
Тенант*	<div>Main</div>
Тип*	<div>kata/edr</div>
Описание	<div></div>

Файлы аутентификации

Вы можете указать пользовательский сертификат и закрытый ключ или автоматически сгенерировать новый самоподписанный сертификат и закрытый ключ

Файл сертификата* 	<div>✓ cert.pem </div>
Закрытый ключ*	<div>✓ key.pem </div>

Создать

Отмена

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.

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

Транспорт

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры

Дополнительные параметры

Коннектор

Создать

Тип*



kata/edr



Подробные сведения о получении событий от Kaspersky Endpoint Detection and Response см. [в онлайн-справке](#).



Для подтверждения параметров интеграции вам нужно принять запрос на подключение от Kaspersky Unified Monitoring and Analysis Platform в веб-интерфейсе Kaspersky Endpoint Detection and Response. Подробнее см. [в онлайн-справке](#).

URL*



10.68.85.13:443



Добавить

Секрет*

KEDR (API)

Внешний ID*



fe11af61-5dfe-4d4b-a263-f7bf3a6ca703

Сохранить

Отмена

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**.

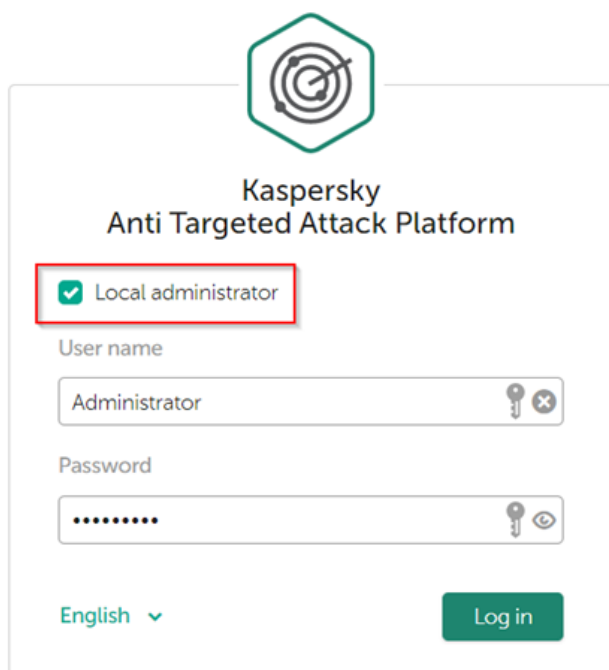
5. Скопируйте появившуюся команду для установки коллектора KUMA.

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**



The image shows the login interface of the Kaspersky Anti Targeted Attack Platform. At the top is a green hexagonal logo with a target symbol. Below it, the text "Kaspersky Anti Targeted Attack Platform" is displayed. A red rectangular box highlights the "Local administrator" checkbox, which is checked. Below this are input fields for "User name" (containing "Administrator") and "Password" (masked with dots). At the bottom left is a language selector set to "English" with a dropdown arrow, and at the bottom right is a green "Log in" button.

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.

External systems

Certificate fingerprint 58:25:6A:69:90:5B:53:F2:1A:8C:67:67:23:F5:C5:89:45:08:78:1C:E4:34:4B:D6:0F:32:59:33:14:9E:48:83
Maximum scan priority ☐ Disabled

Server list

IP/name	Type	Name	ID	Certificate fingerprint	State	
10.68.85.15	External system	KWTS	c5d04e9f-0be8-491f-8a88-661d5193cf54	Certificate fingerprint	Authorized	Delete
10.68.85.16	Kaspersky mail sensor	—		Certificate fingerprint	Authorized	Delete
10.16.58.65	External system	System 34	185b6bd7-ee09-4cb8-933d-24016b3b8150	Certificate fingerprint	Authorized	Delete
10.68.85.45	External system	System fe11af61-5dfe-4d4b-a263-f7bf3a6ca703	fe11af61-5dfe-4d4b-a263-f7bf3a6ca703	Certificate fingerprint	Pending	Accept Reject

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 #11

Created 22 January 2024 08:15:26 by lithium

Updated 16 October 2024 13:02:22 by Boris RZR