

Kaspersky EDR Expert (on-premise) + KUMA standalone: ??? ? ??? ????? ???????????

“ Разбор сценария, когда Kaspersky EDR Expert 8 (развёрнут в Open Single Management Platform (OSMP), а Kaspersky SIEM (KUMA) установлена **отдельно** (standalone). Какие данные KEDR может отдать во внешнюю KUMA, как настроить каждый канал и что в итоге получится на стороне KUMA.

Дата обновления: 01.10.2026

1. ?????? ?????????????????? ???????????????

В KEDR в составе OSMP разворачиваются сервисы KUMA: **Ядро, Коллектор, Коррелятор и Хранилище**. Именно они принимают и обрабатывают EDR-телеметрию:

- телеметрию от агентов (KES в режиме встроенного агента EDR) принимает предустановленный коллектор [00TB] Kaspersky EDR ;
- коррелятор применяет правила [00TB] EDR IOA alert , [00TB] EDR IOA SB alert , [00TB] OSMP Scanner detects и формирует корреляционные события, из которых KEDR создаёт алерты;
- нормализованные события хранятся в хранилище KUMA и доступны в разделе **Мониторинг → Поиск угроз**.

Ресурсы и сервисы этого встроенного движка доступны в консоли OSMP: **Мониторинг → Ресурсы и сервисы → Активные сервисы**. Поэтому выгрузка во внешнюю KUMA строится на штатном механизме KUMA: к коллектору или коррелятору KEDR добавляется **точка назначения** (destination), которая пересылает события во внешний коллектор.

2. ?????? ??????????: ??? ?????? ??????????????

№	Что отправляем	Откуда в KEDR	Как	Чем принимает KUMA standalone
---	----------------	---------------	-----	-------------------------------

1	EDR-телеметрия (нормализованные события с хостов: процессы, файлы, реестр, сеть, DNS и т. д.)	Коллектор [00TB] Kaspersky EDR	Точка назначения tcp (TLS, разделитель \n, JSON)	Коллектор: коннектор tcp (TLS) + нормализатор json + хранилище
2	Корреляционные события (основа алертов: сработки IOA, Sandbox, сканера OSMP)	Коррелятор KEDR8	Точка назначения в маршрутизации коррелятора (tcp / http / kafka)	Коллектор с соответствующим коннектором + json
3	События Сервера администрирования и управляемых приложений (обнаружения KES, статусы устройств, события задач, изменения политик)	Сервер администрирования (KSC в составе OSMP)	Экспорт в SIEM-систему: Syslog или CEF (формат Kaspersky SIEM)	Коллектор [00TB] KSC (CEF / Syslog TCP)

“ Важно: на момент написания статьи, реагирование через KEDR из KUMA не работает.

3. ????? 1. EDR?????????? ?? ??????????? KEDR ?? ???????? KUMA

Это основной сценарий: Отправка событий из коллектора OSMP в коллектор внешней SIEM-системы».

3.1. ?????????????????????????????????

1. Вход в консоль OSMP под учётной записью с правами **Главного администратора**.
2. В OSMP установлен коллектор [00TB] Kaspersky EDR.
3. В KUMA standalone создан и установлен коллектор со следующими ресурсами:
 - коннектор типа **tcp** с включённым режимом **TLS** и разделителем \n;
 - нормализатор типа **json** без сопоставления полей, с сохранением сырого события;
 - точка назначения типа **storage**.

3.2. ??? 1. ????????????????????????????? KUMA standalone

В веб-интерфейсе KUMA: **Ресурсы → Коллекторы → Добавить коллектор**.

1. **Подключение источников:** название (например, KEDR8-telemetry-in) и тенант.

2. **Транспорт:** коннектор → **Создать**, тип **tcp**:
 - **URL** — порт приёма, например `0.0.0.0:5140` (или `<FQDN>:<порт>`);
 - **Разделитель** — `\n`;
 - вкладка «Дополнительные параметры» → **Режим TLS** — **Включено** (или «Нестандартный PFX», если используете сертификат своего УЦ).
3. **Парсинг событий:** нормализатор типа **json**, без сопоставления полей; в параметре **Сохранить исходное событие** выберите **Всегда** — тогда полное событие из KEDR8 сохранится в поле `Raw`.
4. **Маршрутизация:** точка назначения **storage** (хранилище). Если планируете строить собственную корреляцию в KUMA standalone, добавьте также точку назначения **correlator**.
5. **Проверка параметров** → **Сохранить и создать сервис**, скопируйте команду установки и выполните её на сервере коллектора. Откройте порт на межсетевом экране.

3.3. ??? 2. ???????????? ? ????? ??? ?????????? ?????????? (OSMP)

1. **Параметры** → **Тенанты** → тенант **Root** → **Параметры** → **Сертификаты**.
2. Отметьте TLS-сертификат и нажмите **Экспортировать**, задайте пароль. Скачается файл PFX.
3. Распакуйте сертификат и ключ:

```
openssl pkcs12 -in certificate.pfx -clcerts -nokeys -out cert.pem && \
openssl pkcs12 -in certificate.pfx -nocerts -nodes -out key.pem
```

(пароль от PFX нужно ввести дважды).

3.4. ??? 3. ?????? ????????????? tcp ?? ????????????? [00TB]

Kaspersky EDR

1. **Мониторинг** → **Ресурсы и сервисы** → **Активные сервисы** → выберите коллектор `[00TB] Kaspersky EDR`.
2. В окне редактирования коллектора откройте вкладку **Маршрутизация** → **Добавить**.
3. Создайте точку назначения:
 - вкладка «Основные параметры»: **Тип** — `tcp`; **URL** — `<имя_хоста_коллектора_KUMA>:<порт_коллектора_KUMA>`;
 - вкладка «Дополнительные параметры»: **Режим TLS** — **Включено**; **Разделитель** — `\n`;
 - **Сохранить**.
4. Вкладка **Проверка параметров** → **Сохранить и перезапустить сервисы**.



При включённом TLS в поле URL **нельзя указывать IP-адрес** — только имя хоста (FQDN). Позаботьтесь о DNS-записи для коллектора KUMA standalone.

Полезные параметры точки назначения tcp (вкладка «Дополнительные параметры»):

- **Выходной формат** — `JSON` (по умолчанию для этого сценария), также доступны `CEF` и `Syslog-CEF`;
- **Сжатие** — `Snappy` или `gzip`: снижает нагрузку на канал;
- **Дисковый буфер** (по умолчанию включён, 10 ГБ) — события копят на диске, если внешняя KUMA недоступна; при переполнении новые события перезаписывают самые старые;
- **Политика выбора URL** — при нескольких адресах (несколько коллекторов KUMA): «Любой», «Сначала первый» или «Сбалансированный»;
- **Фильтр** — отправлять во внешнюю KUMA **не весь поток**, а только нужные события (например, только определённые `EventType`, только события с признаком IOA, только серверы). Это главный инструмент управления объёмом.

3.5. ??? 4. ????????? ???????

1. **Активные сервисы** → правой кнопкой по `[00TB] Kaspersky EDR` → **Развернуть** → скопируйте **Connector gateway URL**.
2. Отправьте тестовое событие:

```
curl -w "%{http_code}\n" -X POST \  
  --cert cert.pem \  
  --key key.pem \  
  -H "Content-Type: application/json" \  
  --data-binary $'{"Product":"EDR","HostOsFamily":"Test_send_to_external_SIEM_collector"}\n' \  
  https://<Connector gateway URL> -k
```

Ожидаемый ответ — код **200**.

3.6. ??? 5. ????????? ? KUMA standalone

События → найдите событие со значением `Test_send_to_external_SIEM_collector` в поле `KL_HostOsFamily`. В поле `Raw` будет полное событие KEDR8 примерно такого вида:

```
{  
  "ID": "fca85cda-...",  
  "Timestamp": 1776534533425,  
  "TenantID": "d22648f7-...",  
  "ServiceName": "[00TB] Kaspersky EDR",  
  "DeviceTimeZone": "+03:00",
```

```

"Type": 1,
"Extra": { "Product": "EDR" },
"S": {
  "KL_HostOsFamily": "Test_send_to_external_SIEM_collector",
  "KL_Product": "EDR"
}
}

```

3.7. ??? ?????????? ?? ?????? 1

- **Поток уже нормализованных событий KEDR** в формате модели событий KUMA (JSON): поля схемы KUMA, служебные поля (`TenantID`, `ServiceName`), а также EDR-специфичные поля в расширенной схеме (`S.KL_*`, например `KL_HostOsFamily`, `KL_Product`).
- По составу это те же типы событий, что агент отправляет в KEDR: `Process`, `File *`, `Registry *`, `Connection`, `DNS`, `Module`, `Code Injection`, `Process Access`, `Threat Detect`, `Bits Job *`, `Service *`, `Scheduled Task *` и другие (модель данных событий EDR Expert).
- Что это даёт в KUMA standalone: **единое хранилище** EDR-телеметрии рядом с остальными источниками SOC (сеть, AD, СЗИ), **собственные правила корреляции** поверх EDR-данных и других источников, дашборды и отчёты, **длительное хранение** по политикам хранилища KUMA standalone, ретроспективный поиск.

4. ????? 2. ?????????????????????? ?????????? ?? ????????????????? KEDR

Коррелятор KUMA (и встроенный в KEDR тоже) на шаге **Маршрутизация** позволяет указать, куда отправлять созданные им корреляционные события. Обычно это хранилище, но, при необходимости, события можно отправлять в другие места. Точек назначения может быть несколько»*.

Как настроить:

1. **Мониторинг → Ресурсы и сервисы → Активные сервисы** → откройте коррелятор KEDR8.
2. Вкладка **Маршрутизация → Добавить точку назначения → Другое**.
3. Создайте точку назначения типа **tcp** (аналогично каналу 1: FQDN коллектора KUMA standalone, TLS, `\n`, JSON). Также доступны **http** и **kafka**.
4. Сохраните и перезапустите сервис.
5. В KUMA standalone поднимите отдельный коллектор (tcp + json + storage), чтобы корреляционные события лежали отдельно от сырой телеметрии.

Что получаем: корреляционные события, на основе которых KEDR формирует алерты: сработки IOA ([00TB] EDR IOA alert), обнаружения Sandbox ([00TB] EDR IOA SB alert), детекты OSMP Scanner (YARA, IOC, Anti-Malware) и т. п. Объем этого канала на порядки меньше телеметрии, поэтому он хорошо подходит, когда во внешнюю KUMA нужны **только «сигналы»**, без всего потока событий.

“ **Важно.** В KUMA standalone приходят **корреляционные события, а не алерты как объекты**: статусы, назначение аналитика, инциденты и плейбуки остаются в OSMP.

5. ?????? 3. ????????? ????????? ???????????????????????? (Syslog / CEF)

В состав KEDR входит Сервер администрирования (KSC). Он умеет экспортировать в SIEM события, которые хранит в своей базе: события управляемых приложений (например, обнаружения KES), события Сервера, статусы устройств, а также события изменения политик.

5.1. ?????????? ?????????? ? OSMP

1. В главном окне нажмите на **имя Сервера администрирования** → вкладка **Общие** → раздел **Экспорт в SIEM-систему** → **Параметры**.
2. Укажите:
 - **Адрес сервера SIEM-системы и Порт** — адрес коллектора KUMA standalone;
 - **Протокол** — `TCP`, `UDP` или `TLS over TCP` (для TLS настройте аутентификацию сервера: доверенные сертификаты или отпечатки SHA1, при необходимости — клиентский сертификат);
 - **Формат данных — Kaspersky SIEM (KUMA)** (это CEF по правилам `siem_conversion_rules.xml`) или **Syslog** (RFC 5424; для него задаётся максимальный размер сообщения, по умолчанию 2048 байт).
3. При необходимости задайте **дату начала экспорта**: тогда уйдут и архивные события из базы с этой даты.
4. Включите **Экспортировать события в SIEM**.
5. При необходимости включите **Экспорт расширенных событий для изменений политики в SIEM**. События изменения политик **не хранятся** в базе Сервера и доступны **только через SIEM**.
6. **Проверить подключение** → **Сохранить**.

5.2. ?????? ?????????? ????????

- **Формат Kaspersky SIEM (CEF)** — экспортируются **все общие события**, выбирать их нельзя.

- **Формат Syslog** — уходят **только события, отмеченные для экспорта**. Если ничего не отмечено, не уйдёт ничего. Отметить можно:
 - общие события: имя Сервера или политика → **Настройка событий** → **Отметить для экспорта в SIEM-систему по протоколу syslog**;
 - события конкретного приложения: **Управление активами** → **Политики** → политика приложения → **Настройка событий** → отметить события → **Отметить для экспорта в SIEM-систему по протоколу syslog**;
 - события для конкретного устройства: **Активы (Устройства)** → устройство → **Приложения** → приложение → **Настройка событий**. Если события уже выбраны в политике, переопределить их для отдельного устройства нельзя.

5.3. ????? ? KUMA standalone

Ресурсы → **Коллекторы** → коллектор с нормализатором `[00TB] KSC` (CEF, Syslog TCP):

1. **Транспорт** — порт, совпадающий с указанным в OSMP.
2. **Парсинг событий** — нормализатор `[00TB] KSC`.
3. **Маршрутизация** — точки назначения **Хранилище** и **Коррелятор**.
4. **Сохранить и создать сервис** → установите коллектор командой из веб-интерфейса.

Что получаем: события KES и Сервера администрирования (обнаружения угроз, результаты обработки, статусы защиты, события задач и политик) в нормализованном виде. Это «ЕРР-слой» данных: он хорошо дополняет EDR-телеметрию из канала 1, а аудит изменений политик возможен **только** через этот канал.

Revision #2

Created 6 October 2026 05:27:45 by Анна

Updated 6 October 2026 06:10:09 by Анна