

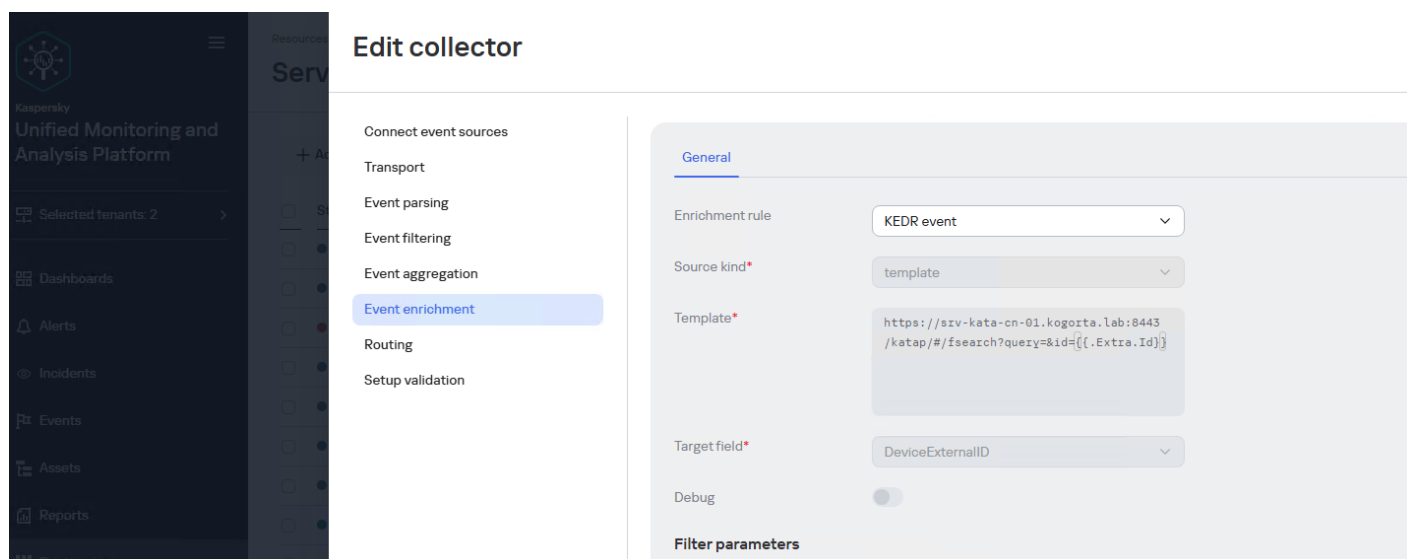
# ???????????????????? KEDR 7.1 ?????????? ?? ???????

Скорее всего есть нюансы с распределенными инсталляциями KATA/KEDR. Не проверялось.

Правило работает аналогично правилу обогащения [OOTB] KATA alert.

- Правило: [правило обогащения телеметрии KEDR.kuma](#)
- Пароль на ресурс: `q123123Q!KLaapt-M4`

1. Добавить правило обогащения на коллектор, который собирает телеметрию KEDR.



2. Найти интересующее событие в KUMA

**Kaspersky**  
Unified Monitoring and Analysis Platform

Selected tenants: 2

- Dashboards
- Alerts
- Incidents
- Events**
- Assets
- Reports
- Resources
- Task manager

## Events

No refr

```
1 SELECT * FROM `events` WHERE ServiceID = '87d6c9c1-c00
```

Press Ctrl + Enter to run query

### Query results

TSV

TenantID	Timestamp	Name
Main	2026-02-26 13:45:47.540	File change
Main	2026-02-26 13:45:47.540	File change
Main	2026-02-26 13:45:47.539	25
Main	2026-02-26 13:45:47.539	Registry change
Main	2026-02-26 13:45:47.539	Registry change
Main	2026-02-26 13:45:47.539	Registry change
Main	2026-02-26 13:45:47.538	File change
Main	2026-02-26 13:45:47.538	Registry change

## Event details

Copy

TenantID	Main
SpaceID	KUMA Default
Timestamp	2026-02-26 13:45:47.540
Name	File change
EndTime	2026-02-26 13:45:00.788
Message	File PrsCADB.tmp was create on srv-endpoint-01.kogorta.lab
DeviceAction	create
DeviceAddress	192.168.76.150
DeviceEventCategory	filechange
DeviceExternalID	<a href="https://srv-kata-cn-01.kogorta.lab:8443/katap/#/fsearch?query=&amp;id=0e5d1e7ae2f99fba3e0ebf25c33915859e89bd89c6e38a3a167caaca63ad9722">https://srv-kata-cn-01.kogorta.lab:8443/katap/#/fsearch?query=&amp;id=0e5d1e7ae2f99fba3e0ebf25c33915859e89bd89c6e38a3a167caaca63ad9722</a>
DeviceHostName	srv-endpoint-01.kogorta.lab
DeviceNtDomain	kogorta.lab
DeviceProduct	EDR

### 3. Перейти по ссылке в KATA/KEDR

**Kaspersky**  
Anti Targeted Attack Platform

- Мониторинг
- Алерты 1
- События в трафике сети
- Поиск угроз**
- Задачи
- Политики
- Пользовательские прав...
- Хранилище
- Активы
- Карта сети
- Риски и аномалии
- Отчеты

## Изменен файл

Изолировать srv-endpoint-01.kogorta.lab
Создать правило запрета
Создать задачу

Создан файл	Инициатор события
Файл: "C:\Users\Administrator.KOGORTA\AppData\Local\Temp\PrsCA...	Файл: "C:\Windows\System32\rdpclip.exe"
MD5: d41d8cd98f00b204e9800998ecf8427e	Параметры запуска: rdpclip
SHA256: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855	Найти события
Тип файла: Неизвестно	MD5: 267675fab6680c07d539b00489942a93
Размер: -	SHA256: 42f7192da2c30f70c4b2b908bc1b1db4e3e1eee958e313c075da695c6040f059

Revision #2

Created 2026-05-27 13:16:43 UTC by Boris RZR

Updated 2026-05-27 13:23:00 UTC by Boris RZR