Настройка обнаружения DLL hijacking

?????????, ??????????? ?? ?????? ????????, ???????? ??????????? ??????? pre-sales ?/??? community KUMA ? **НЕ** ???????? ??????????? ????????????? ???????.

??????????? ???????????? ?? ??????? ??????? ????????? ? ??????-??????? ?? ???????: https://support.kaspersky.ru/kuma/4.2/304384

??? ?????? ???? ??????? KUMA ?????????:

- ???????? ? ??????? AI
- ?????? ?? KSN

???????? ?????????? DLL ???????? ?? ????? ?????????? ???????, ??????? ??? ????? ????????? ???? ?? ??????? ???????? (??????? ???????), ???? ?? ??????? ??????????? (??????????????? ???????). ????????????? ???????????? ????????? ?????, ????????? ?????? ??? ??? ????????? ?????????? ????????? ????????????????????? ? ????????? ?? ??????? KUMA ? KSN

Как это работает с коррелятором:

1. ?? ???????? ????? ???????? Sysmon + KUMA Agent ??? EDR Expert Agent , ??????? ?????????? ?????????? ? KUMA
2. ??????? ??????? ??????????? ?????? (??????? ????, ???? ? ??????, ????? ?????????) ? ?????????? ?? ?????? ??? ???????? ? ???????????
3. ?????????? ????????? ??????? ??????????, ??????? ????????? ??????? ?????????? ? ???????????????? ???????, ??????? ????? ???? ????????????? ????????? ? ??????? KSN
4. KSC ????????? ?????????? ? ?????????? ??????? ???????, ??????? ???????? ? ????

KL_AI_DLLHijackingCheckResult:

- 0- ?? ???????????????. ????? ???????? ??????, ??? ?????????? ???????? ????????? ??????.
- 1 - ??????????. ?? ?????? ????????? ??????? ?????????? ?? ????????? ???????????
- 2 - ?????????????. ??? ????????? ?????? ?????????? ???????? ??????????????, ???? ? ???
- ????????? ???????????????? ??????? ??????????.
- 3 - ??????. ?????? "??????????" ????????? ?? ????? ??????? ??????????? ??????????? ????????? ?????????? DLL, ??? ?????? "?????????????"

Настройка с помощью Agent EDR

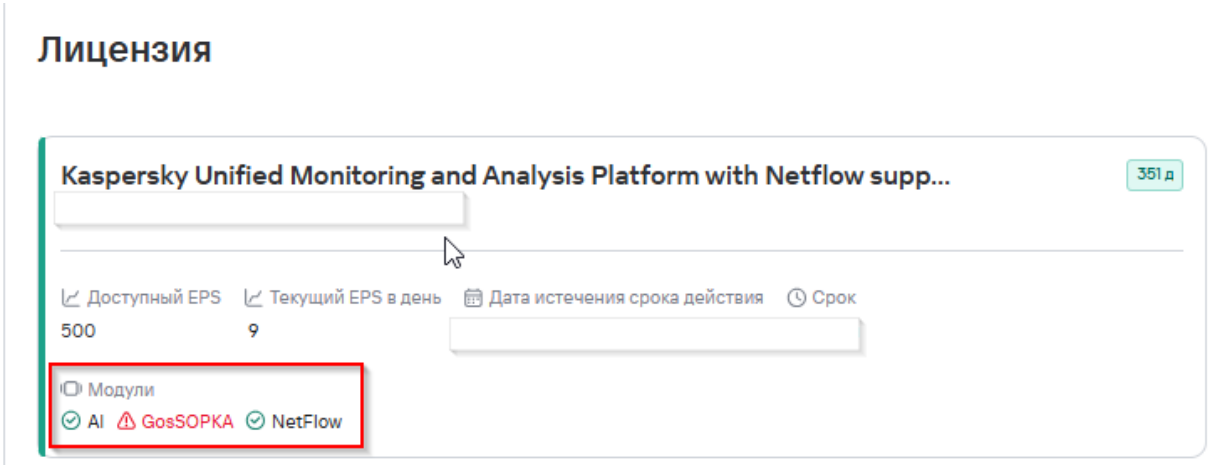
1. ?????????, ??? ? SIEM ????????? ?????????? KEDR

Результаты запроса

TSV

TenantID	Timestamp	Name	DeviceVendor	DeviceAddress	DeviceProduct
Main	02.07.2026 14:40:00.463	File change	Kaspersky	10.68.85.129	EDR
Main	02.07.2026 14:40:00.463	Process	Kaspersky	10.68.85.129	EDR
Main	02.07.2026 14:40:00.463	Process terminate	Kaspersky	10.68.85.129	EDR
Main	02.07.2026 14:40:00.463	File change	Kaspersky	10.68.85.129	EDR
Main	02.07.2026 14:40:00.463	Process	Kaspersky	10.68.85.129	EDR
Main	02.07.2026 14:40:00.463	Process	Kaspersky	10.68.85.129	EDR
Main	02.07.2026 14:40:00.463	Process	Kaspersky	10.68.85.129	EDR

2. ???????? KUMA ???????????? ?????? AI

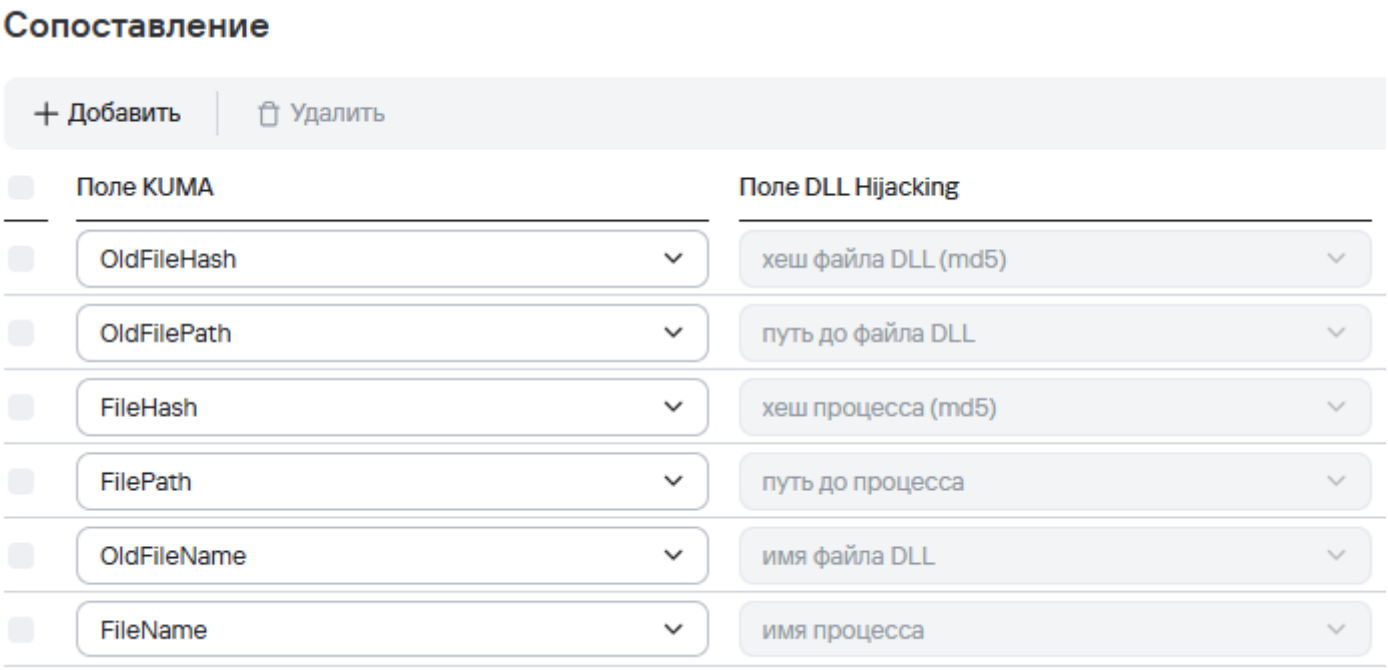


3. ????????? ? **Ресурсы -> Правила Обогащения -> Создать**

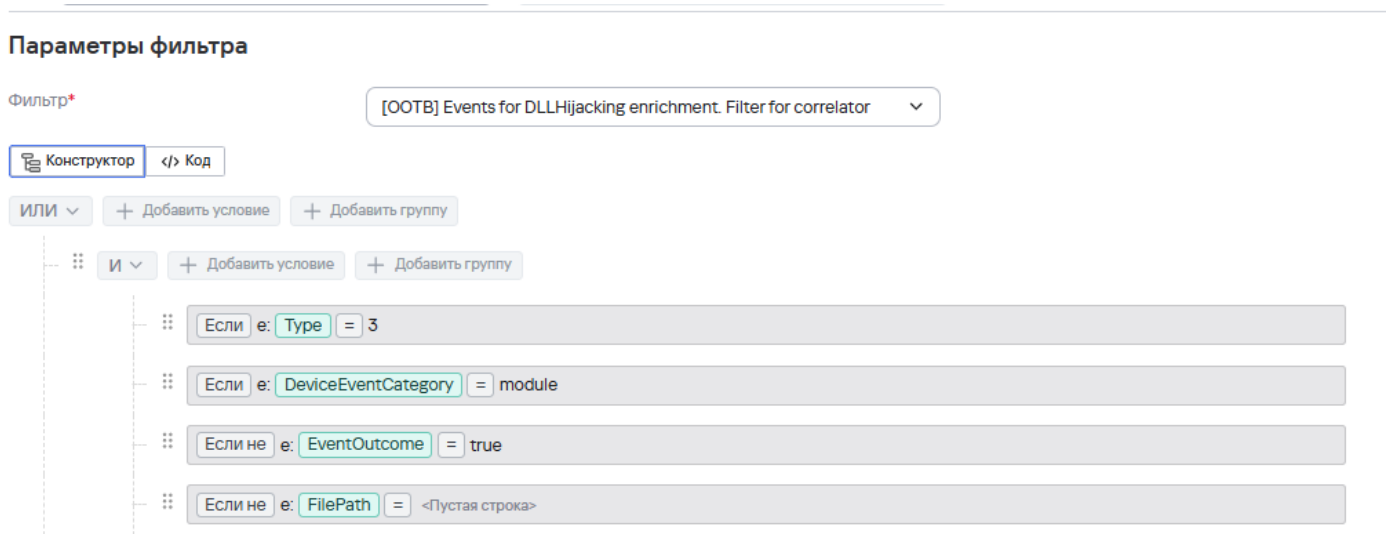
????????? ????:

- ???????? - DLL Hijacking
- ??????
- ??? ????????? ?????? - ???????? DLL Hijacking

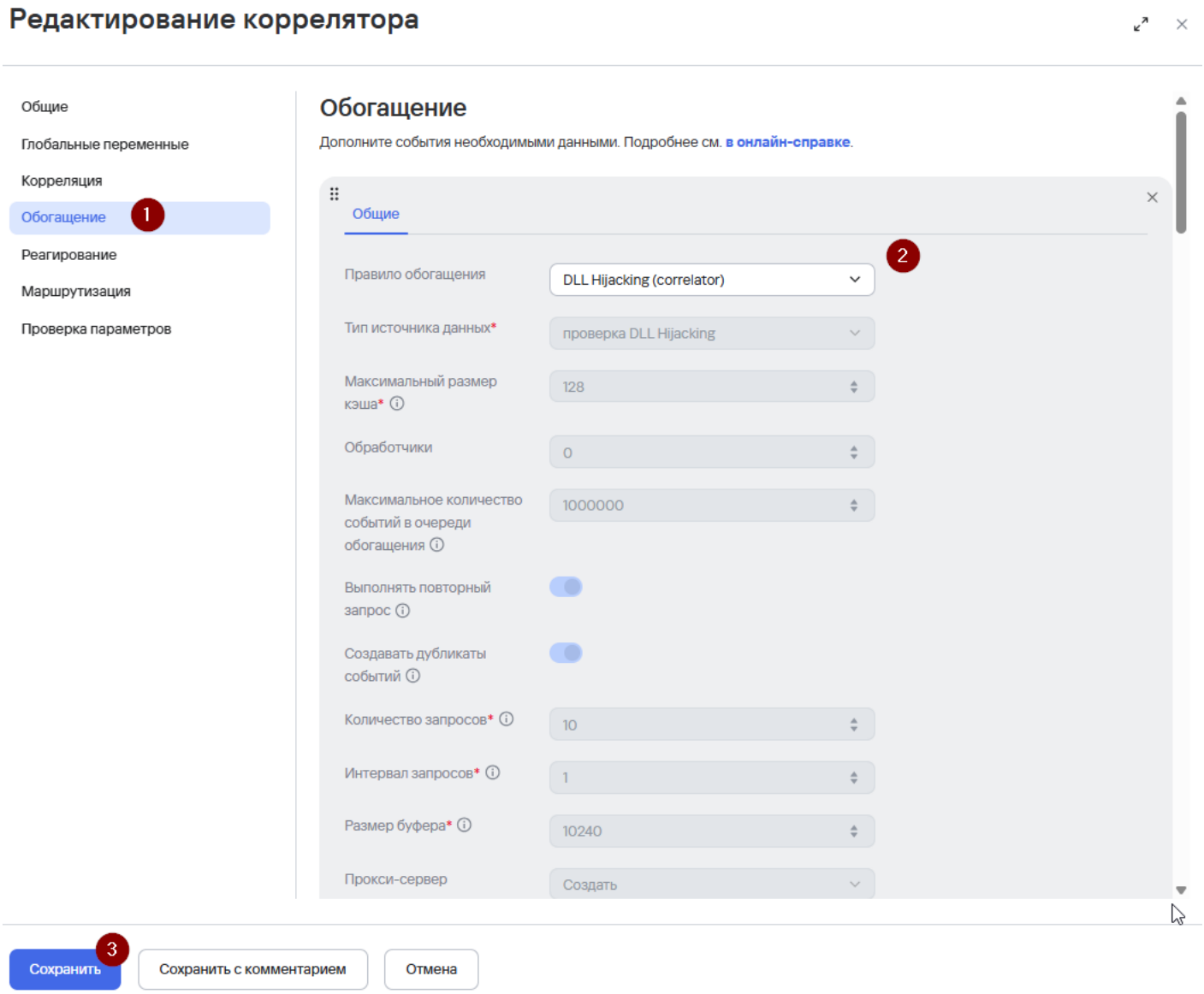
4. ? ??????? **Сопоставление** ? ????????????? ??????? ?????????? ?????????? ???? ???????



5. ? ??????? **Параметры фильтра** ? ????????????? ??????? ?????????? ???????? ?????????? ?????? - **[OOTB] Events for DLLHijacking enrichment. Filter for correlator**



6. ???????? ????????? ??????? ?????????? ?? ?????????? ??? ????? ????????? ? **Ресурсы -> Корреляторы,** ???????? ?????? ? ? ?????????? ?????????????:

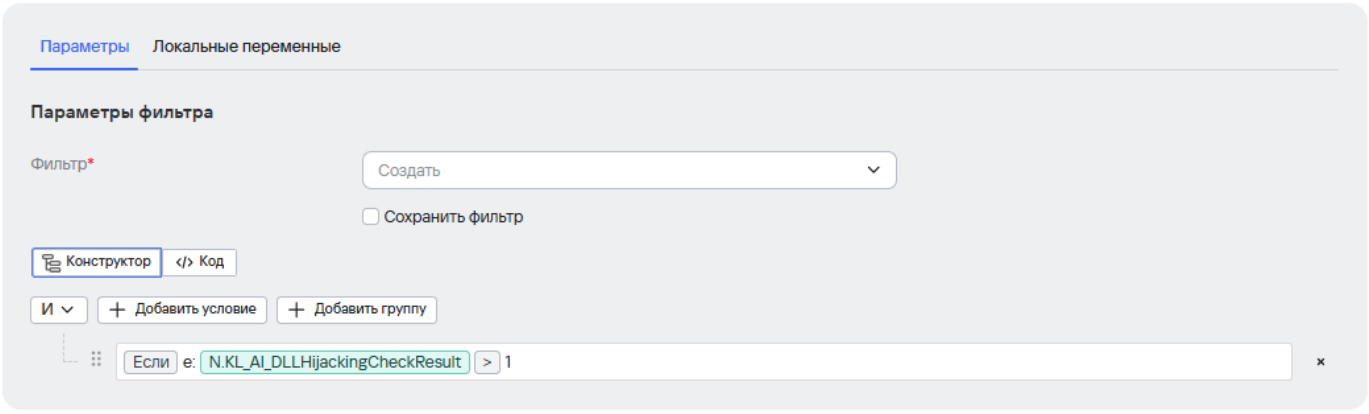


7. ???????? ??????? ?????????? **Ресурсы -> Корреляторы -> Корреляция -> в редактировании коррелятора -> Добавить**

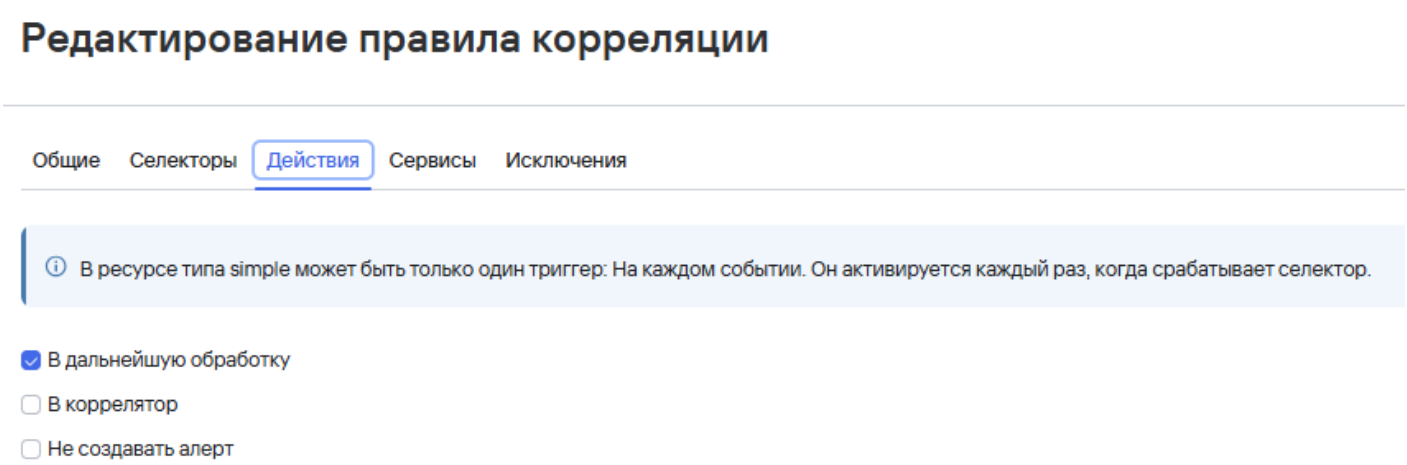
????????? ????????? ? ??????? **Общие**:

- ????????
- ??? - Simple
- ??????????? ???? - FileName
- ??????? ???????? - ???????

? ??????? **Селекторы**:



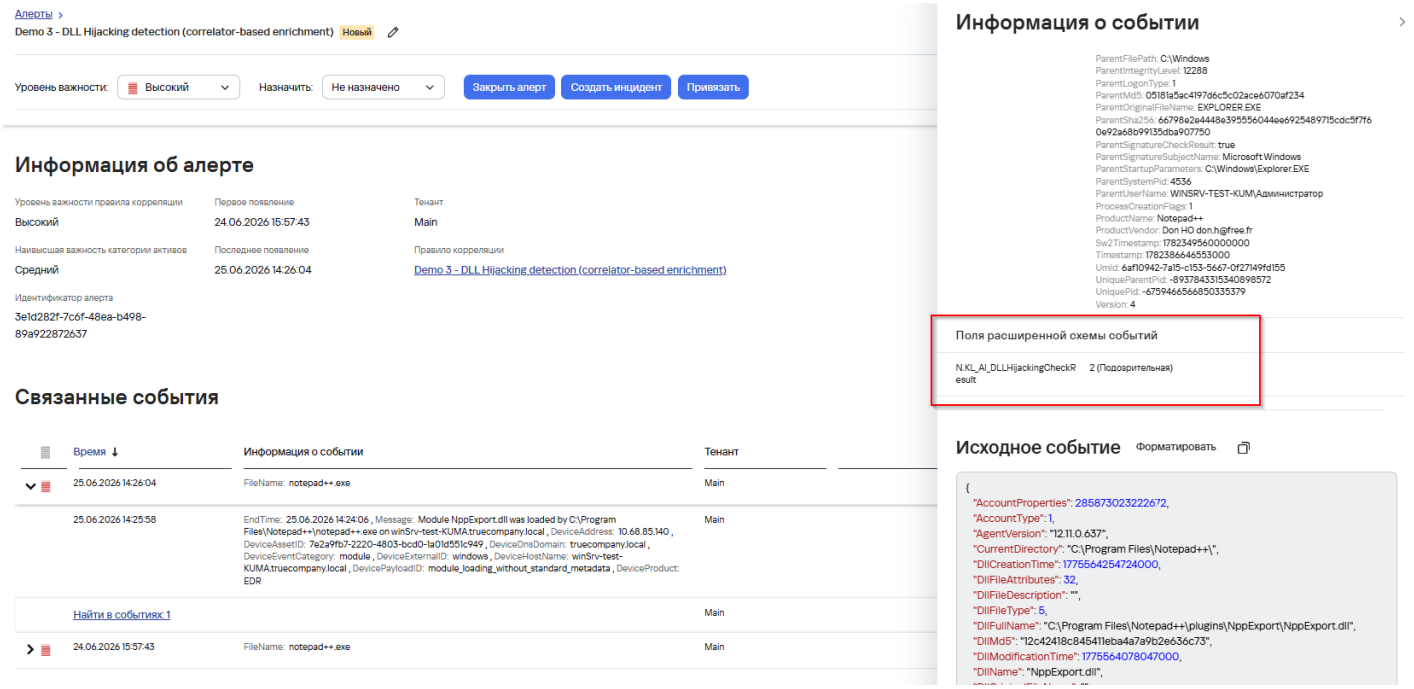
? ??????? **Действия**



? ??????? **Сервисы** ????????? ??????? ?????????? ? ???????????

8. ???????? ????????? ??????????? ????? **Ресурсы -> Активные сервисы**

9. ? ?????????? ??????? ??????????? ?????????? ? ??????? ???????????? ?????, ? ??????? ??????? ?????????? ??????? ? ?????????????



Revision #9

Created 2026-07-02 11:33:08 UTC by lerat

Updated 2026-07-13 10:50:14 UTC by lerat