????????? ???????????? DLL hijacking

> 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.ru/kuma/4.2/304384

Для работы этой функции KUMA требуется:

- Лицензия с модулем AI
- Доступ по KSN

Перехват библиотеки DLL работает во время обогащения событий, поэтому его можно настроить либо на стороне сборщика (базовые события), либо на стороне коррелятора (коррелированные события). Рекомендуется использовать последний метод, поскольку потому что это позволяет эффективно управлять производительностью и нагрузкой на стороны KUMA и KSN

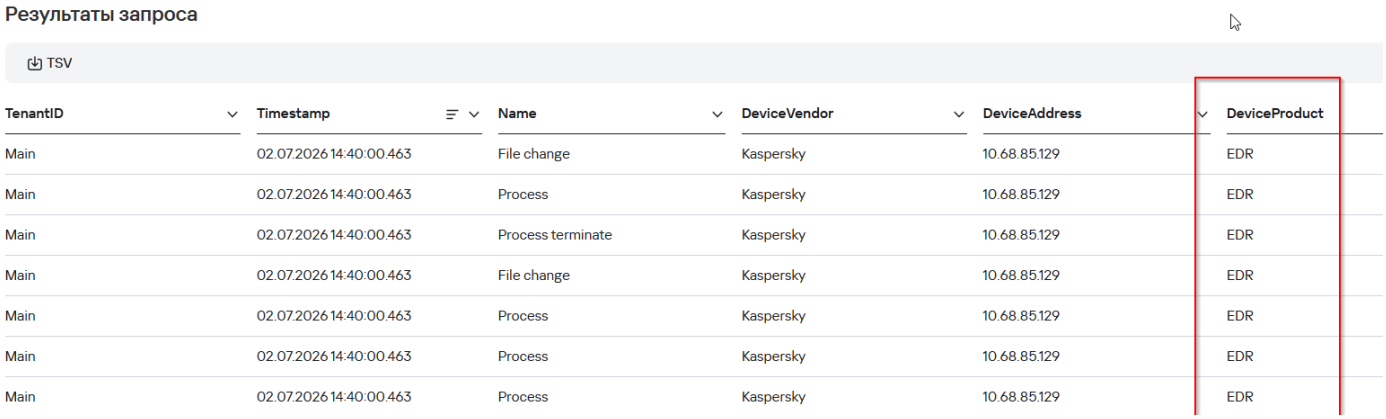
Как это работает с коррелятором:

1. На конечной точке настроен Sysmon + KUMA Agent или EDR Expert Agent , который отправляет телеметрию в KUMA
2. Сборщик успешно нормализует данные (включая хэши, пути к файлам, имена процессов) и пересылает их дальше для хранения и коррелятора
3. Коррелятор запускает правило корреляции, которое запускает событие корреляции с соответствующими данными, которые могут быть дополнительно обогащены с помощью KSN
4. KSC проверяет индикаторы и отправляет обратно вердикт, который хранится в поле **KL_AI_DLLHijackingCheckResult:**

- 0- Не классифицирован. Чтобы получить статус, вам необходимо повторно отправить запрос.
- 1 - Неизвестно. На момент получения статуса библиотека не считается вредоносной
- 2 - Подозрительно. При получении такого результата выдается предупреждение, если у вас
- настроено соответствующее правило корреляции.
- 3 - Ошибка. Статус "Неисправен" указывает на более высокую вероятность обнаружения перехвата библиотеки DLL, чем статус "Подозрительно"

????????? ? ??????? Agent EDR

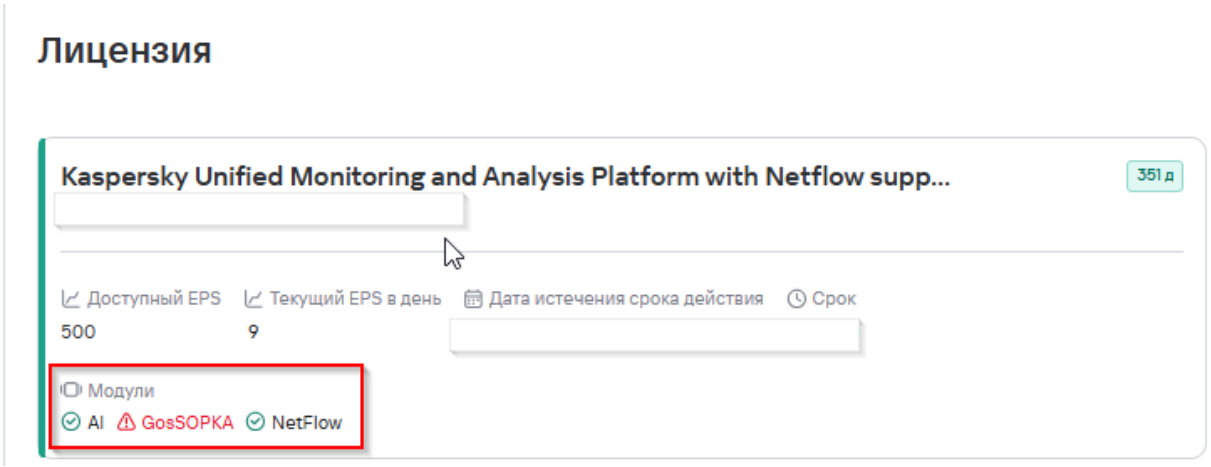
1. Убедитесь, что в SIEM поступает телеметрия KEDR


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. Лицензия KUMA поддерживает модуль AI

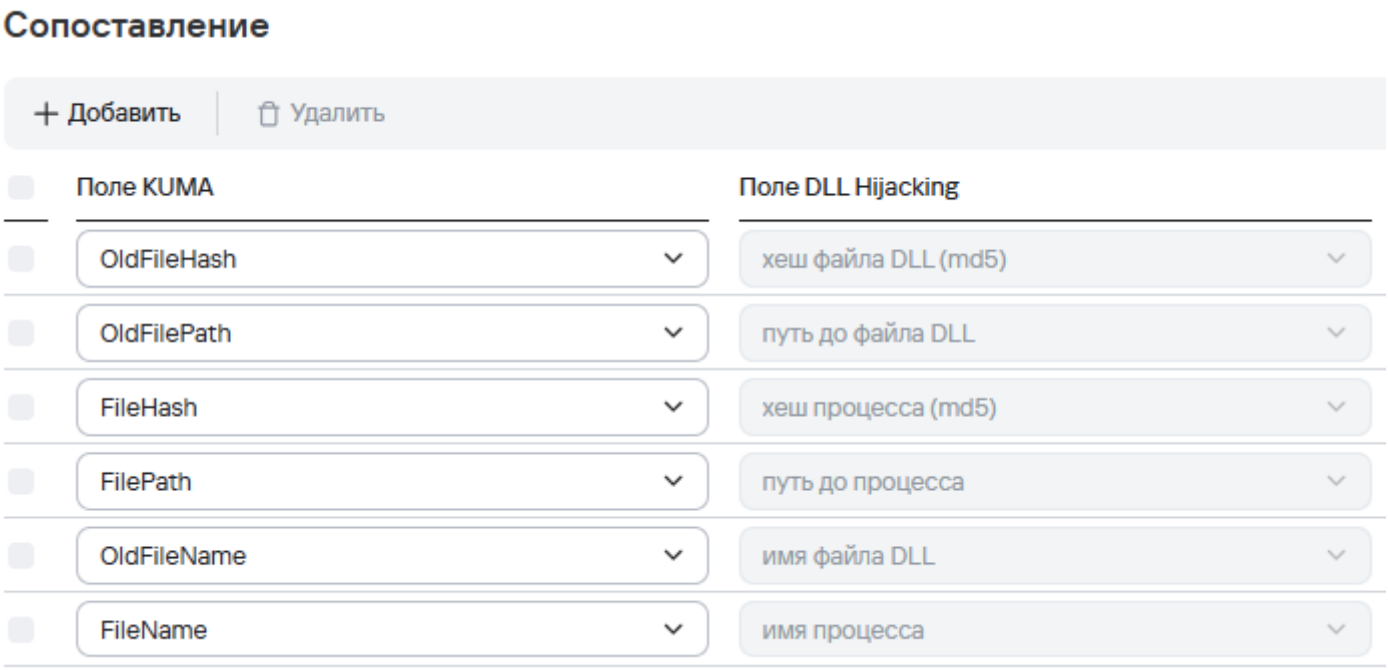


3. Перейдите в **Ресурсы -> Правила Обогащения -> Создать**

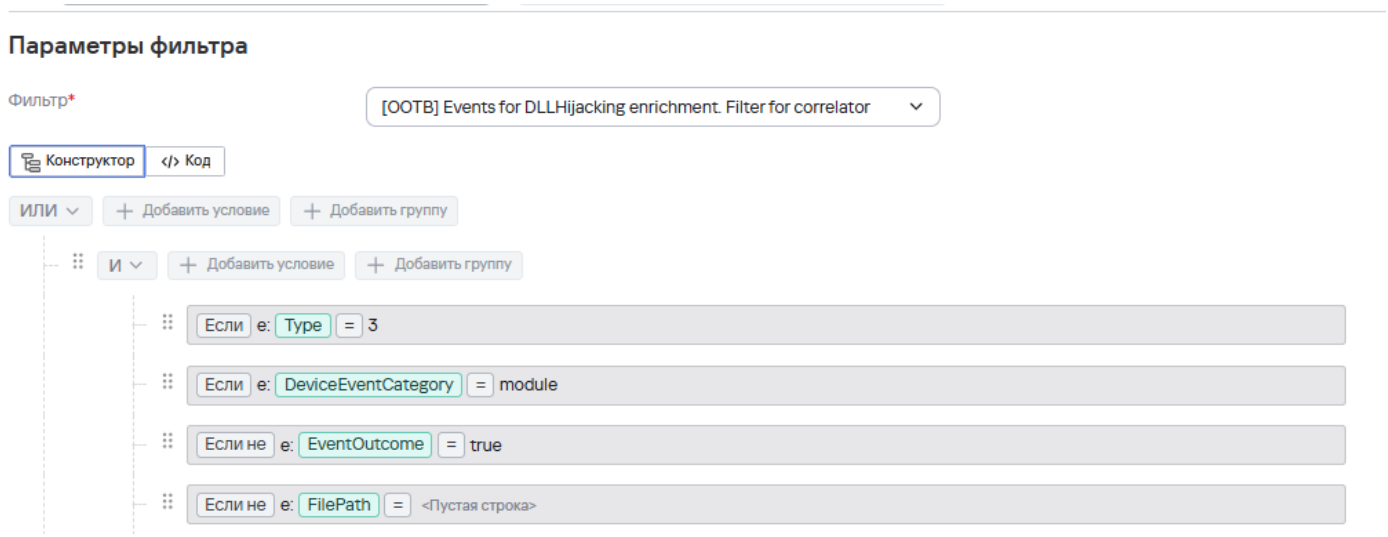
Заполните поля:

- Название - DLL Hijacking
- Тенант
- Тип источника данных - проверка DLL Hijacking

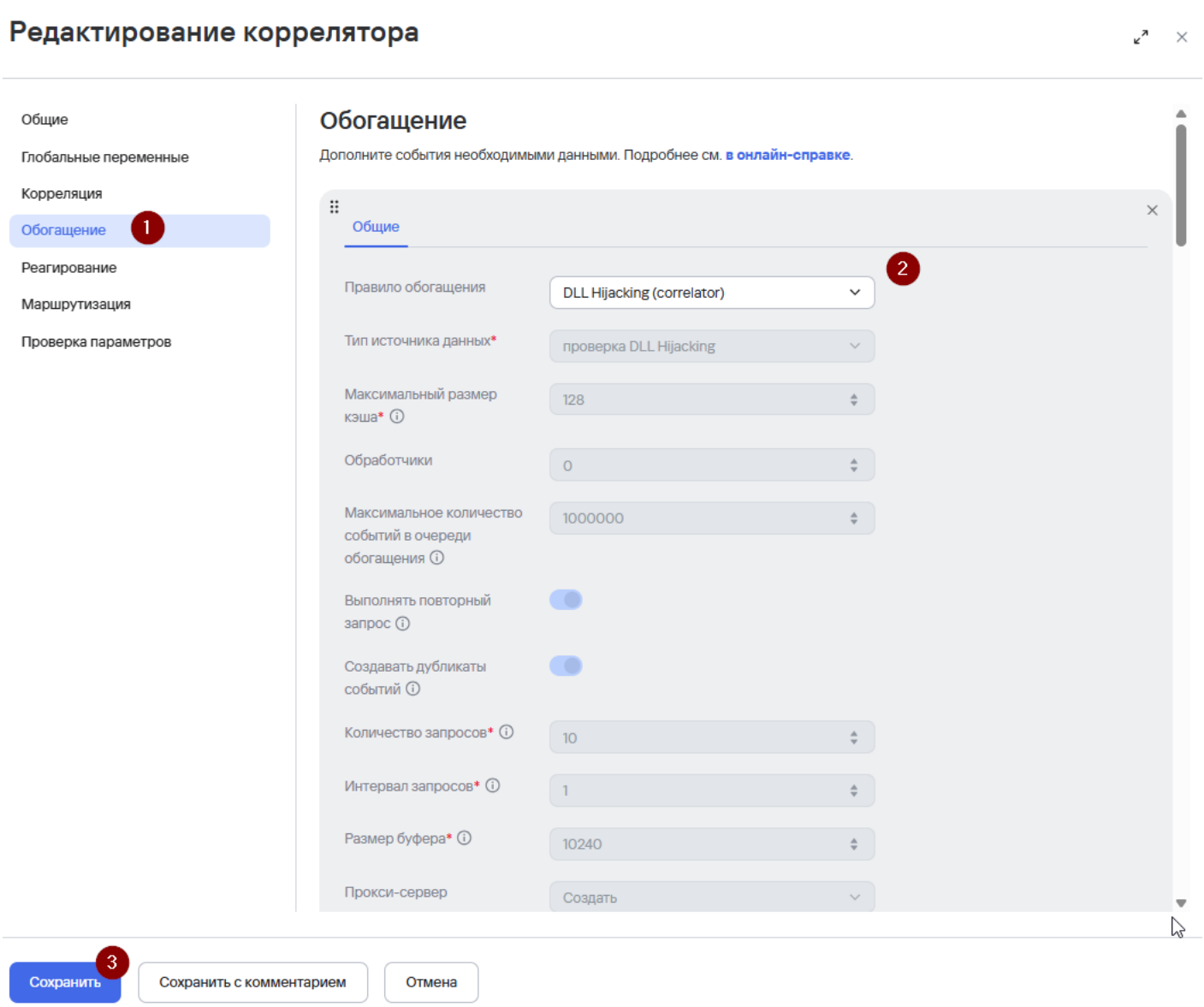
4. В разделе **Сопоставление** в редактировании правила обогащения установите поля событий



5. В разделе **Параметры фильтра** в редактировании правила обогащения выберите коробочный фильтр - **[OOTB] Events for DLLHijacking enrichment. Filter for correlator**



6. Добавьте созданное правило обогащения на коррелятор для этого перейдите в **Ресурсы -> Корреляторы,** откройте нужный и в параметрах редактирования:

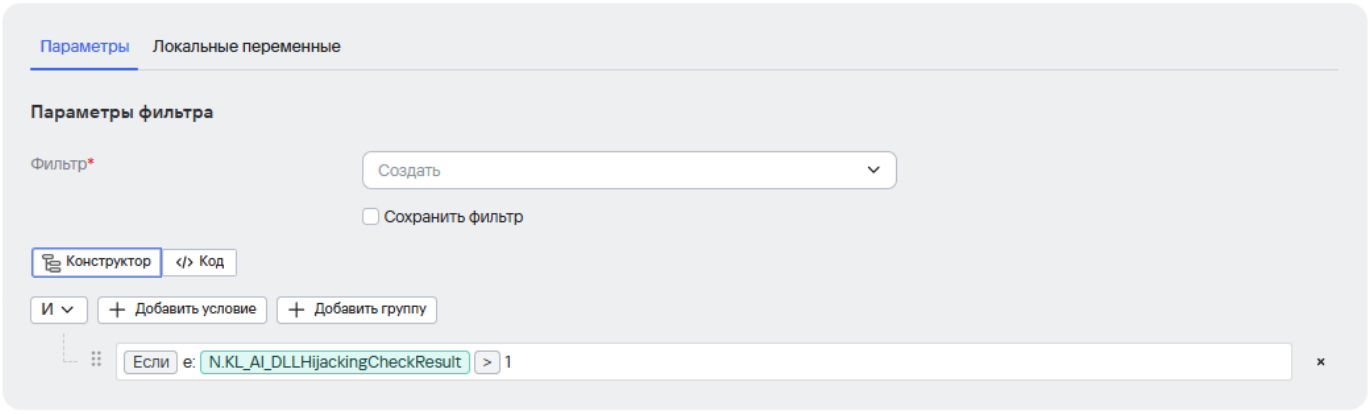


7. Создайте правило корреляции **Ресурсы -> Корреляторы -> Корреляция -> в редактировании коррелятора -> Добавить**

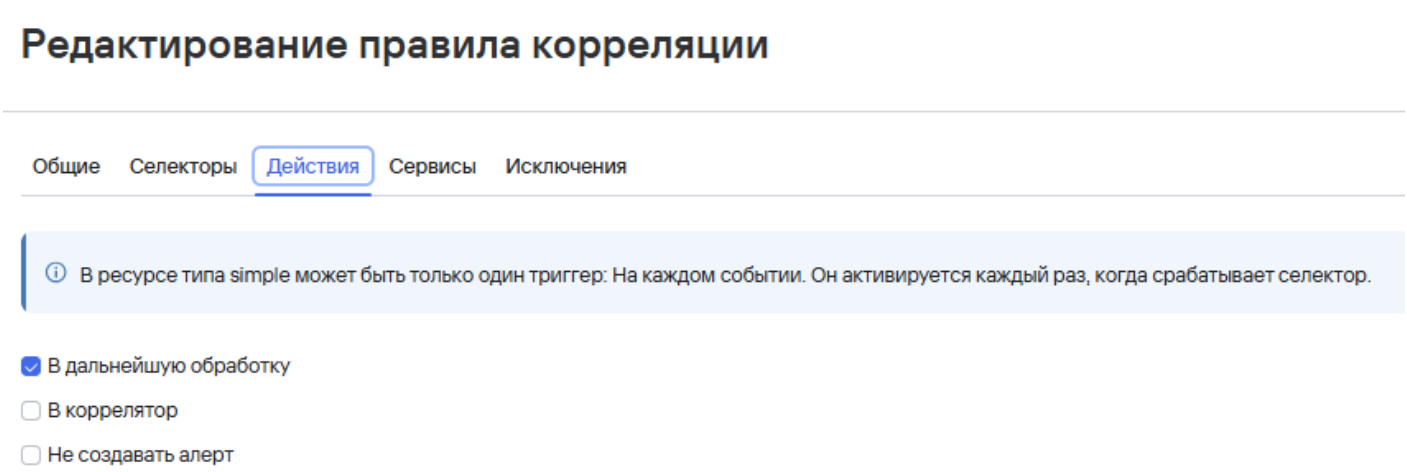
Заполните параметры в разделе **Общие**:

- Название
- Тип - Simple
- наследуемые поля - FileName
- Уровень важности - высокий

в разделе **Селекторы**:



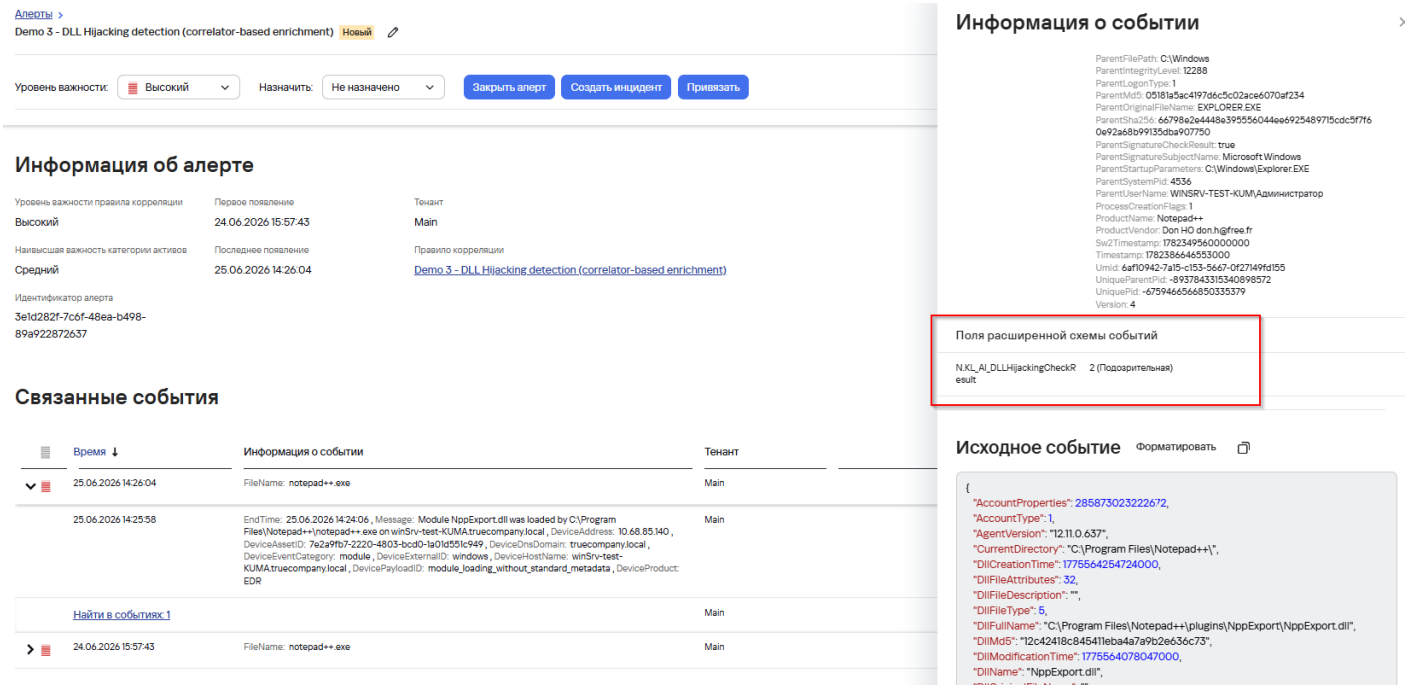
В разделе **Действия**



в разделе **Сервисы** привяжите правило корреляции к коррелятору

8. Обновите параметры коррелятора через **Ресурсы -> Активные сервисы**

9. В результате запуска вредоносной библиотеки в системе сформируется алерт, в базовом событии добавиться вердикт о вредоносности



Revision #8
Created 2026-07-02 11:33:08 UTC by lerat
Updated 2026-07-03 11:30:22 UTC by lerat