Реагирование на алерты и инциденты

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

????? ?? ????? ????????????? ?????? ??? ????????? ???????? ???????????, ???????????? ?? ??????????? (Containment) ??????/????????????? ??? ?????????? (Eradication) ??????.

Сдерживание (Containment)

Цель: ?????????? ?????????????? ??????/????????????? ? ????????????? ?????.

Примеры возможных действий:

- ???????? ?????????? ??????/??????? ?????????/??????.
- ?????????? ??????????? IP-??????? ??? ???????.
- ????????? ?????????? ????????, ???? ??? ??????????.

Устранение (Eradication)

Цель: ????????? ????????? ??????? ?????????.

Примеры возможных действий:

- ???????? ???????????? ?? ??? ??????????? ????????.
- ???????? ???????????, ??????? ???? ???????????? ???????????????.
- ?????????? ?????? ? ?????????? ?? ?????????? ??????.
- ????? ????????????????????? ??????? ?????? (???????, ??????).

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

- ???????????? ????? Kaspersky Security Center:
  - ?????? ?????????? ???????????? ??? ? ??????? Kaspersky Endpoint Security ??? Windows ??? Linux;
  - ?????? ?????? ?????? ???????????? ??.
- ???????????? ????? KEDR:
  - ?????????? ??????? ????????? ???????.

    - ?????????? ????????? ??????? (?? ???-????? ?????).
    - ?????? ?????????.
- ??????????? ????? KICS for Networks:
    - ????????? ??????? ?????????? ?? ???????????
    - ????????? ??????? ?????????? ?? ????????????
- ??????????? ????? Active Directory:
    - ?????????? ??????? ?????? ? ??????.
    - ???????? ??????? ?????? ?? ??????.
    - ????? ?????? ??????? ??????.
    - ?????????? ??????? ??????.
- ?????????? ????????????? ??????? ?? ??????? ???????????? KUMA.

???????? ?? ??????????? ????? ???????????? ??????? ?? ???-?????????? KUMA ??? ????????????? ? ??????? ?????? ????????????.

> ?????? ??????-??????? «?????????? ? ??????? ?????????»
>
> https://support.kaspersky.ru/kuma/4.0/217927

> ?????? KUMA Community «????????????» (???????? «?????????» ?????????? ?? ?????????? ?????????):
>
> https://kb.kuma-community.ru/books/integracii/chapter/reagirovanie

???? ?????????? ?????? ??????? ???????????? ?????????? Kaspersky Security Center.

Создание задач в Kaspersky Security Center

????????????? ????????? ???? ?? ????????? ?????????? ? Kaspersky Security Center, ????????? ? ?????? ?????????? ? Kaspersky Security Center.

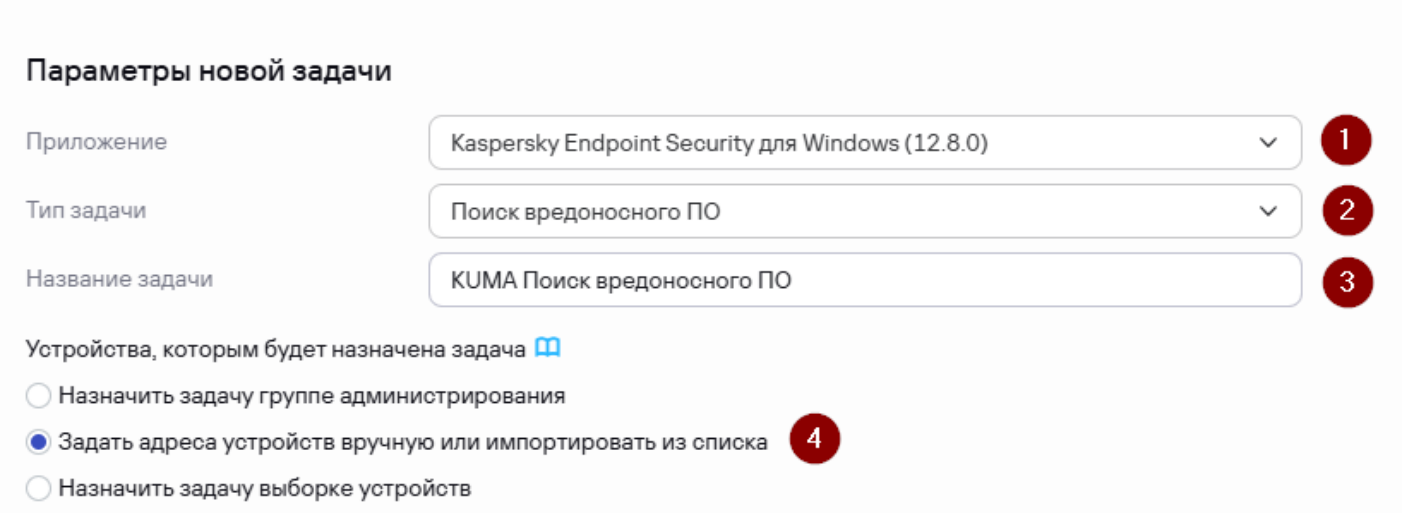
?? ?????? ??????? ??? ????????????? ????????? ?? ??????? Kaspersky Security Center, ????????????? ? KUMA, ?????? ?????????? ???????????? ??? ? ??????? ????????? ? ?????? ?????? ???????????? ??. ?? ??????? ?????? ???? ?????????? ????????? Kaspersky Endpoint Security ??? Windows ??? Linux.

????????????? ?? ??????? Kaspersky Security Center ?????????? ??????? ?????? ?????????? ???????????? ??? ? ?????? ???????????? ??.

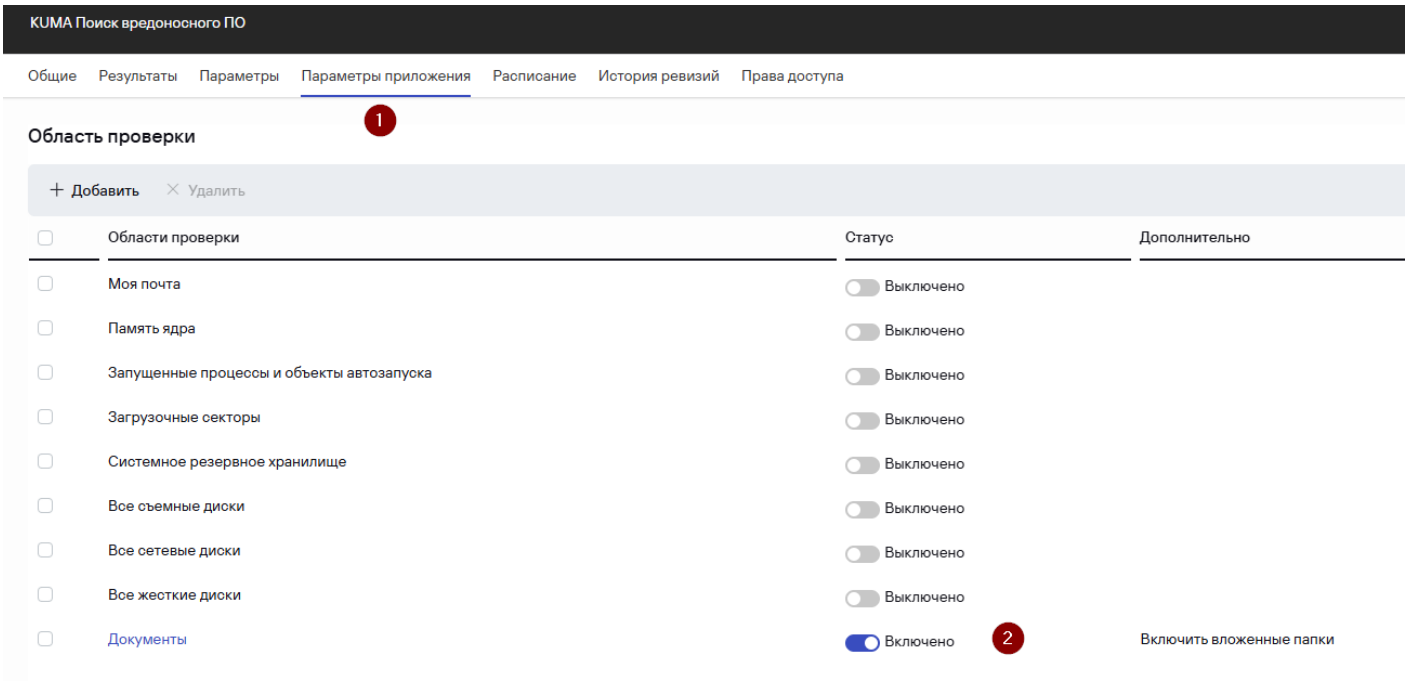
Kaspersky Security Center Web Console

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

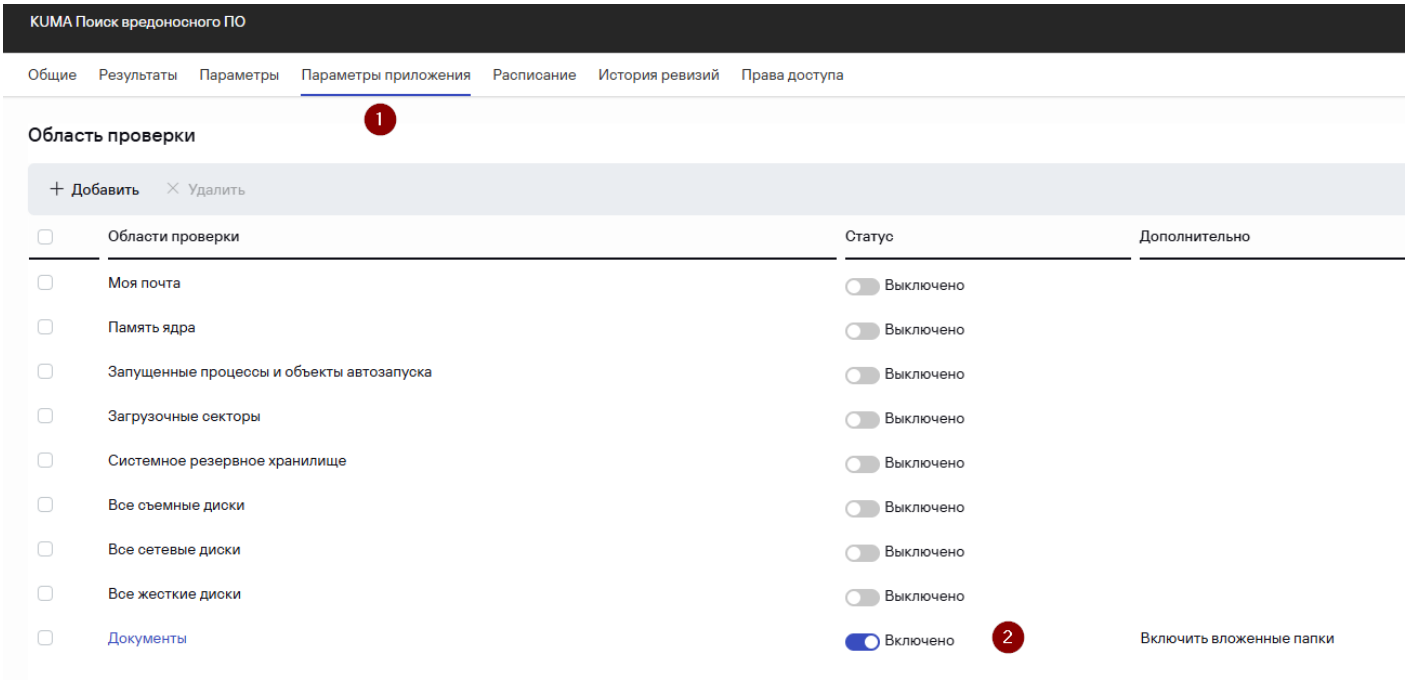
- ???????? **Активы (Устройства)** ? **Задачи**.
- ? ?????? ????? ??????? ?? ?????? **Добавить**.
- ?????????? ?????? ???????? ??????.
- ????????? ????????? ??????:
  - ? ????????????? ?????? **Приложение** ???????? ???????????? ?????????? Kaspersky Endpoint Security ??? Windows (? ????? ??????? 12.8.0).
  - ? ????????????? ?????? **Тип задачи** ???????? **Поиск вредоносного ПО.**
  - ? ???? **Название задачи** ??????? ???????? ??????????? ??????. ????? ? ???????? ?????? ??????? ??????? «**KUMA**». ?????? ??? Kaspersky Endpoint Security ? ?????? ????????? ? ?????????? ????? ???????? ? ?????????? KUMA.
  - ? ????? **Устройства**, **которым будет назначена задача** ???????? **Задать адреса устройств вручную или импортировать из списка.**



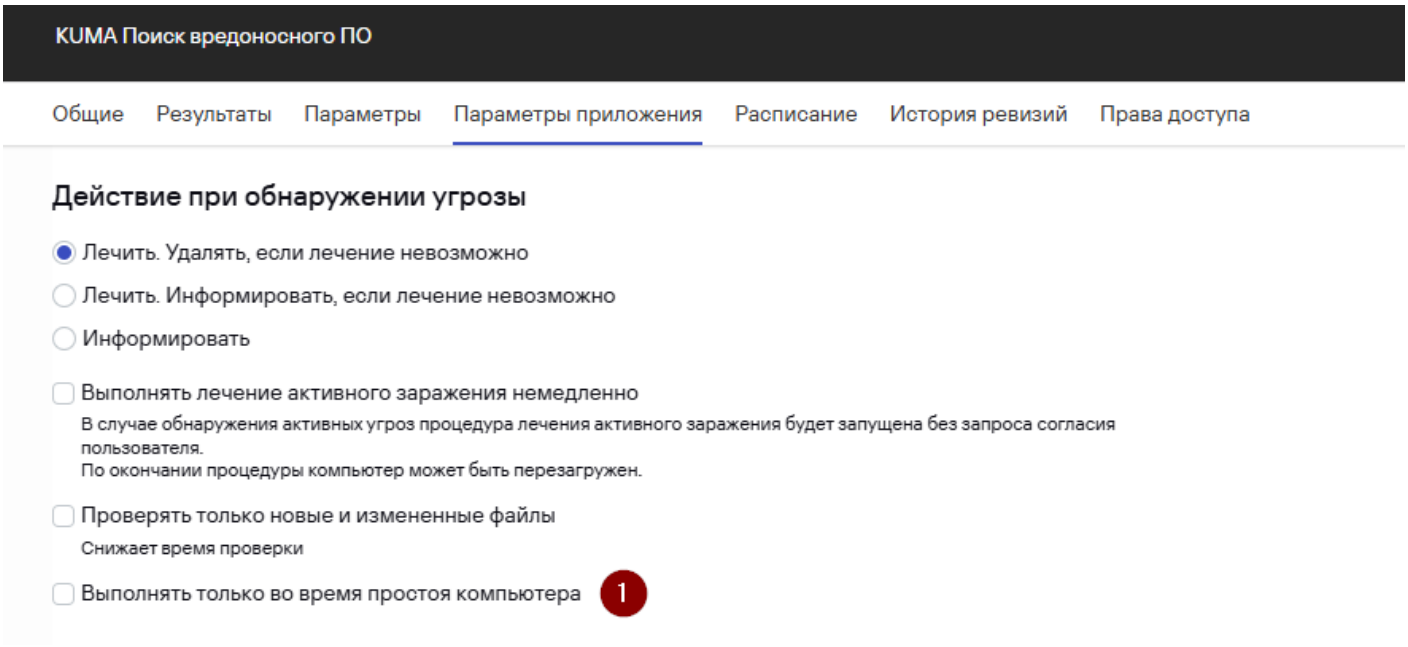
- ??????? ?? ?????? **Далее**.
- ? ???? **Область действия задачи** ??????? **Добавить устройства**. ? ???? ?????? **Добавить устройства** ???????? **Выбрать устройства, обнаруженные в сети Сервером администрирования**. ??? ???????? ?????? ????? ??????? ????? ??????????. KUMA ????? ?????????? ????? ?????????, ?? ??????? ????? ????????? ?????? ?????? ???????????? ??.



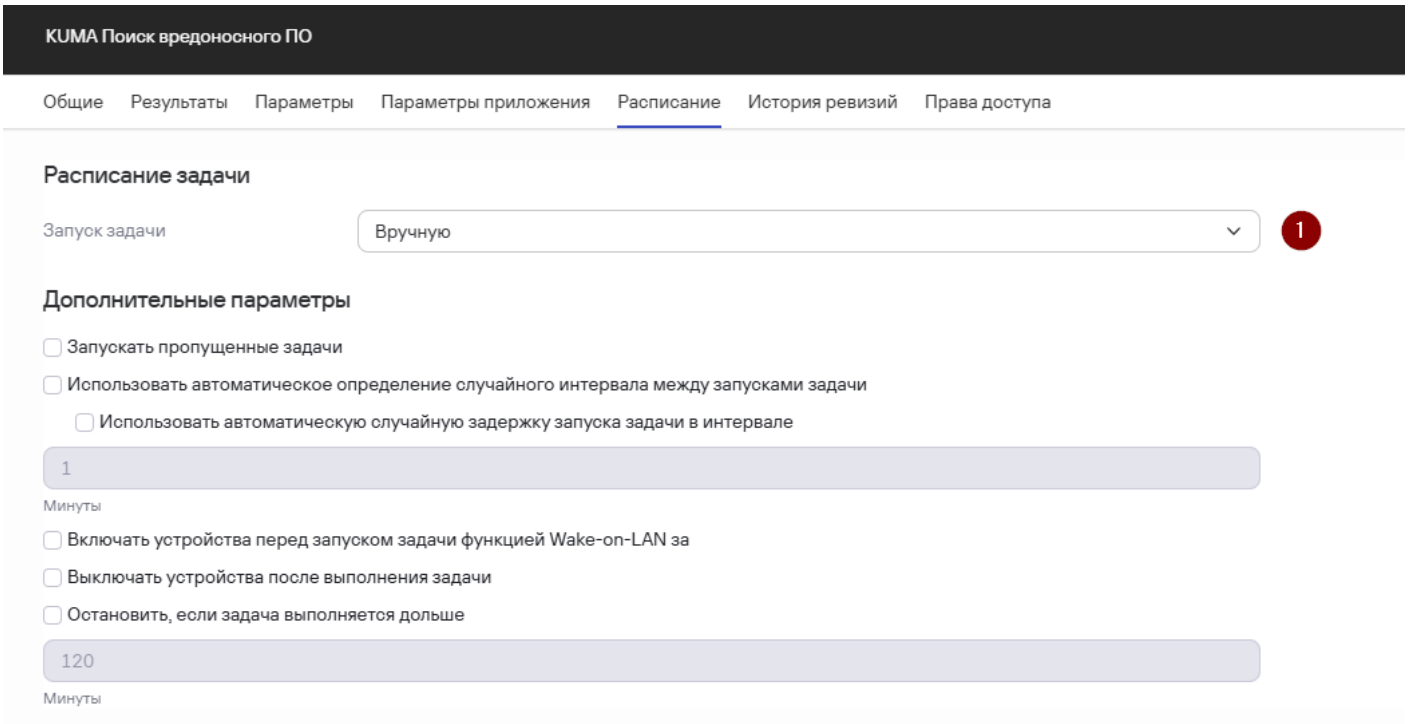
- ??????? **Добавить** ? ????? **Далее**.
- ? ???? **Выбор учетной записи для запуска задачи** ??????? **Учетная запись по умолчанию**. ??????? **Далее**.
- ????????? ?????? ???????, ????? ?????? **Готово**.
- ? ??????????? ???? ??????? ?????? ????????? ?? ??????? **Параметры приложения** ? ??????? **Области проверки**. ? ?????? ???????????? ????? ????????? ??????? ????????. ? ?????????? ??? ????????? ????? ????????.



- ? ?????? **Действие при обнаружении угрозы** ??????? ?????? **Выполнять только во время простоя компьютера**.



- ????????? ?? ??????? **Расписание** ? ?????????, ??? ??? ????????? **Запуск задачи** ??????? **Вручную**.



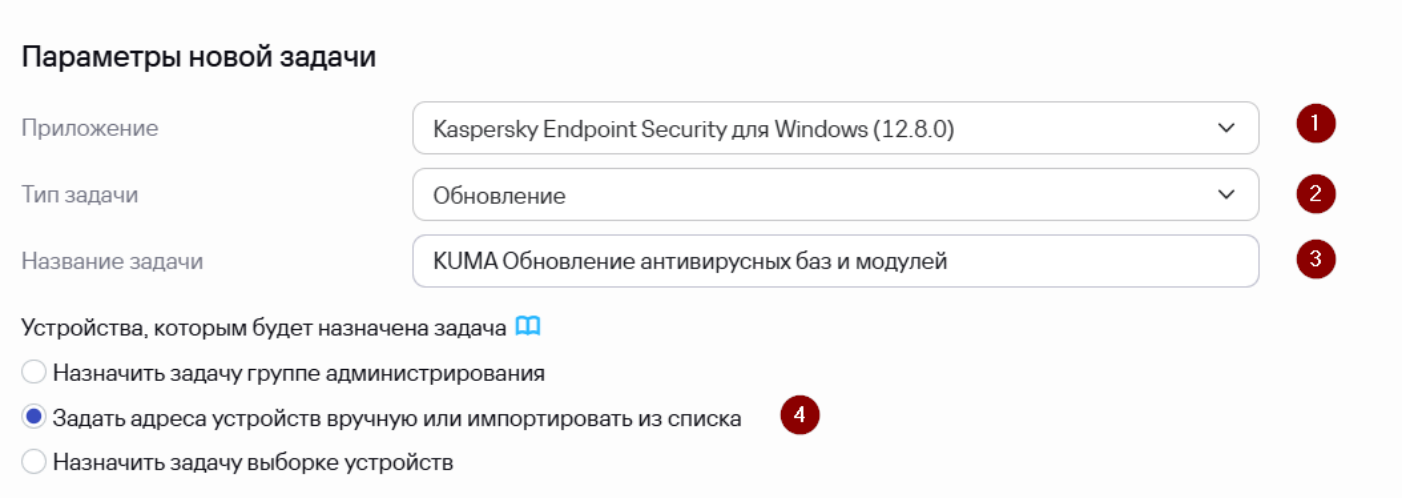
- ??????? **Сохранить**.

?????? ?????? ???????????? ?? ???????.

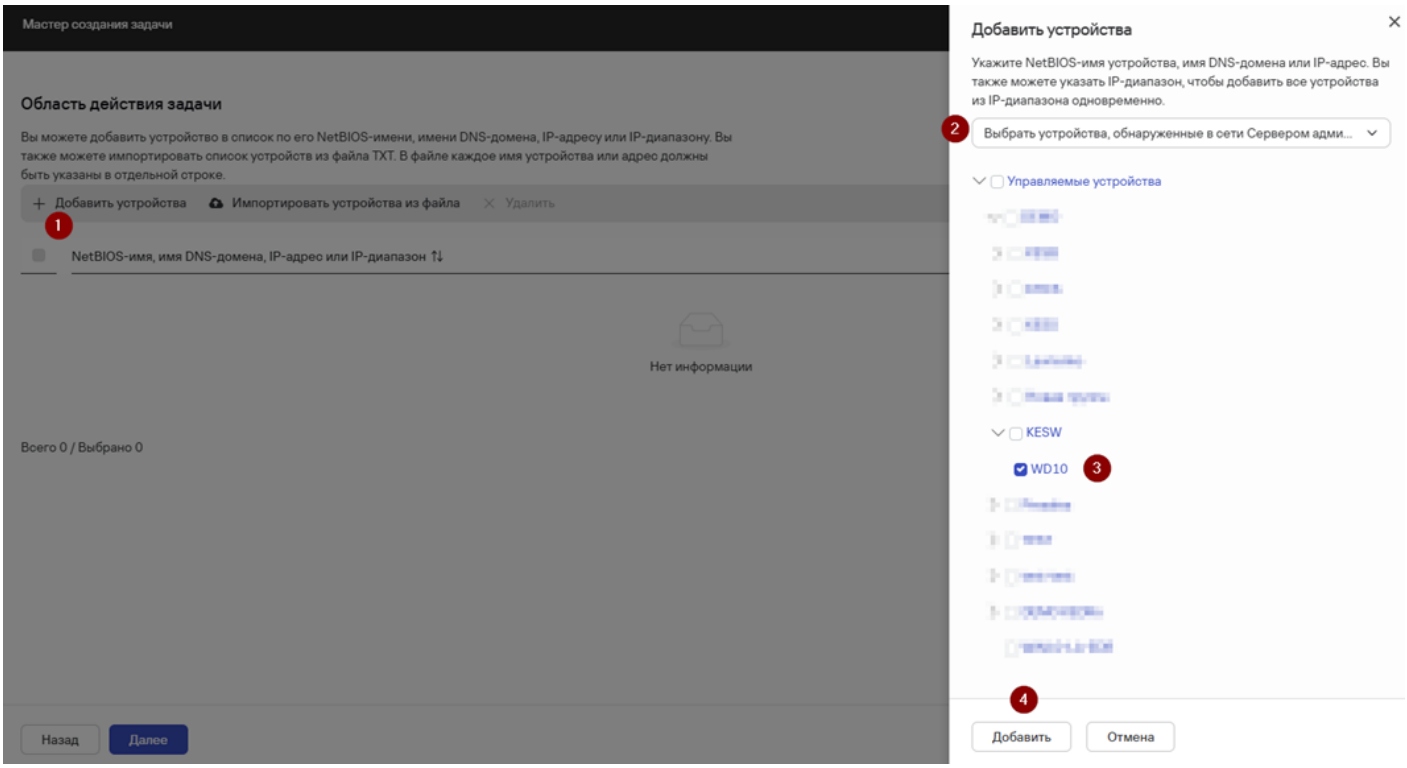
????? ???????? ?????? ?????????? ???????????? ??? ? ???????.

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

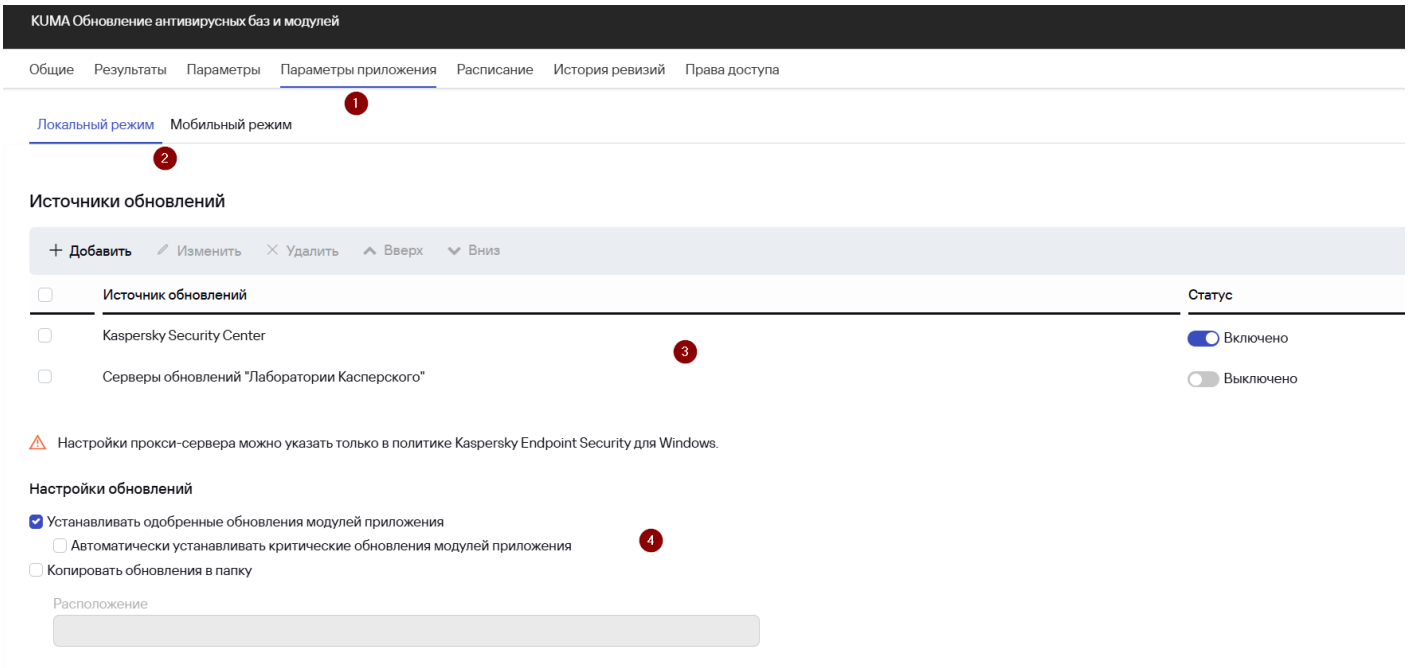
- ???????? **Активы (Устройства)** ? **Задачи**.
- ? **Списке задач** ??????? ?? ?????? **Добавить**
- ?????????? ?????? ???????? ??????.
- ????????? ????????? ??????:
  - ? ????????????? ?????? **Приложение** ???????? ???????????? ?????????? Kaspersky Endpoint Security ??? Windows (? ????? ??????? 12.8.0).
  - ? ????????????? ?????? **Тип задачи** ???????? **Обновление**.
  - ? ???? **Название задачи** ??????? ???????? ??????????? ??????. ????? ? ???????? ?????? ??????? ??????? «**KUMA**». ?????? ??? Kaspersky Endpoint Security ? ?????? ????????? ? ?????????? ????? ???????? ? ?????????? KUMA.
  - ? ????? **Устройства, которым будет назначена задача** ???????? **Задать адреса устройств вручную или импортировать из списка**.



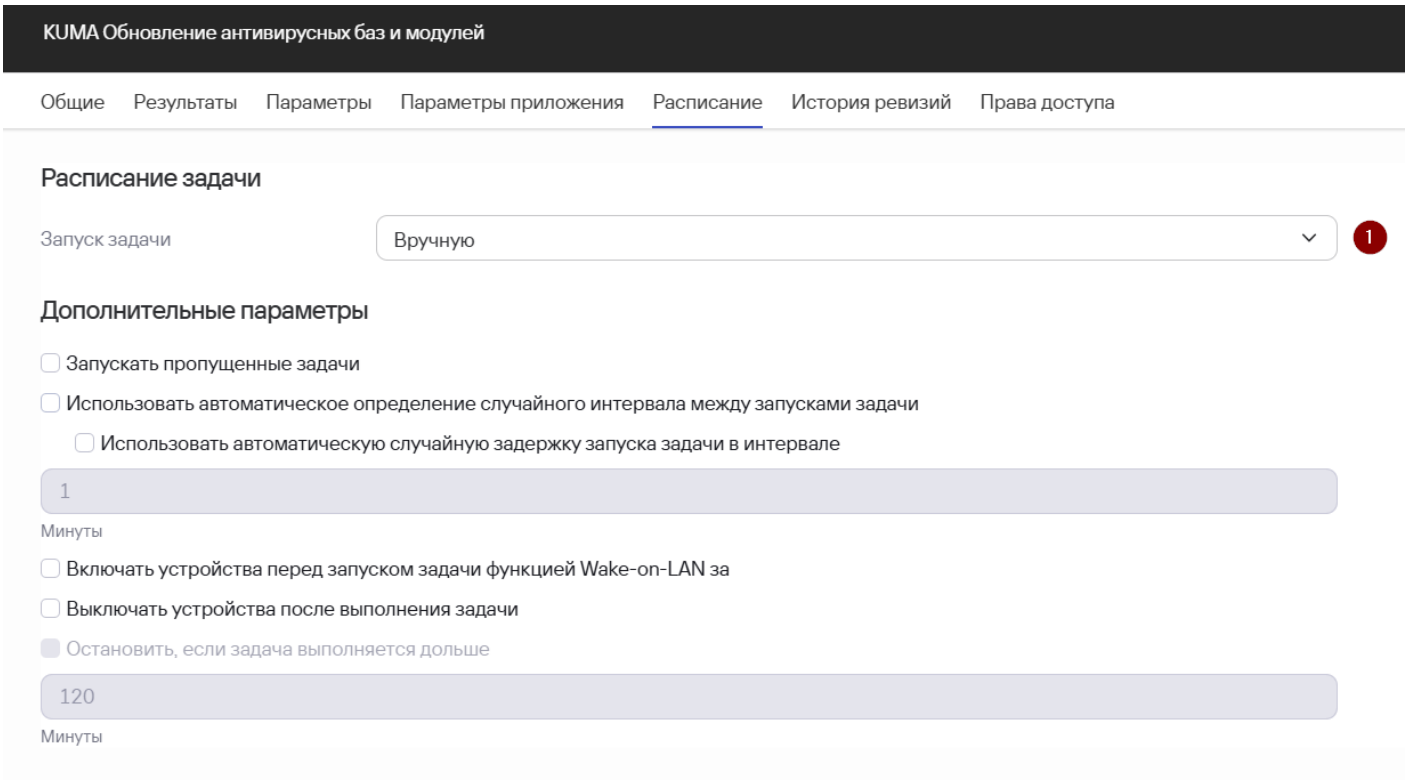
- ??????? ?? ?????? **Далее**.
- ? ???? **Область действия задачи** ??????? **Добавить устройства**. ? ???? ?????? **Добавить устройства** ???????? **Выбрать устройства, обнаруженные в сети Сервером администрирования**. ??? ???????? ?????? ????? ??????? ????? ??????????. KUMA ????? ?????????? ????? ?????????, ?? ??????? ????? ????????? ?????? ?????????? ???????????? ???.



- ??????? **Добавить** ? ????? **Далее**.
- ? ???? **Выбор учетной записи для запуска задачи** ??????? **Учетная запись по умолчанию**. ??????? **Далее**.
- ????????? ?????? ???????, ????? ?????? **Готово**.
- ? ??????????? ???? ??????? ?????? ????????? ?? ??????? **Параметры приложения** ? ??? ????????????? ?????????????? **Источники обновлений** ? **Настройки обновлений.**



- ????????? ?? ??????? **Расписание** ? ?????????, ??? ??? ????????? **Запуск задачи** ??????? **Вручную**.



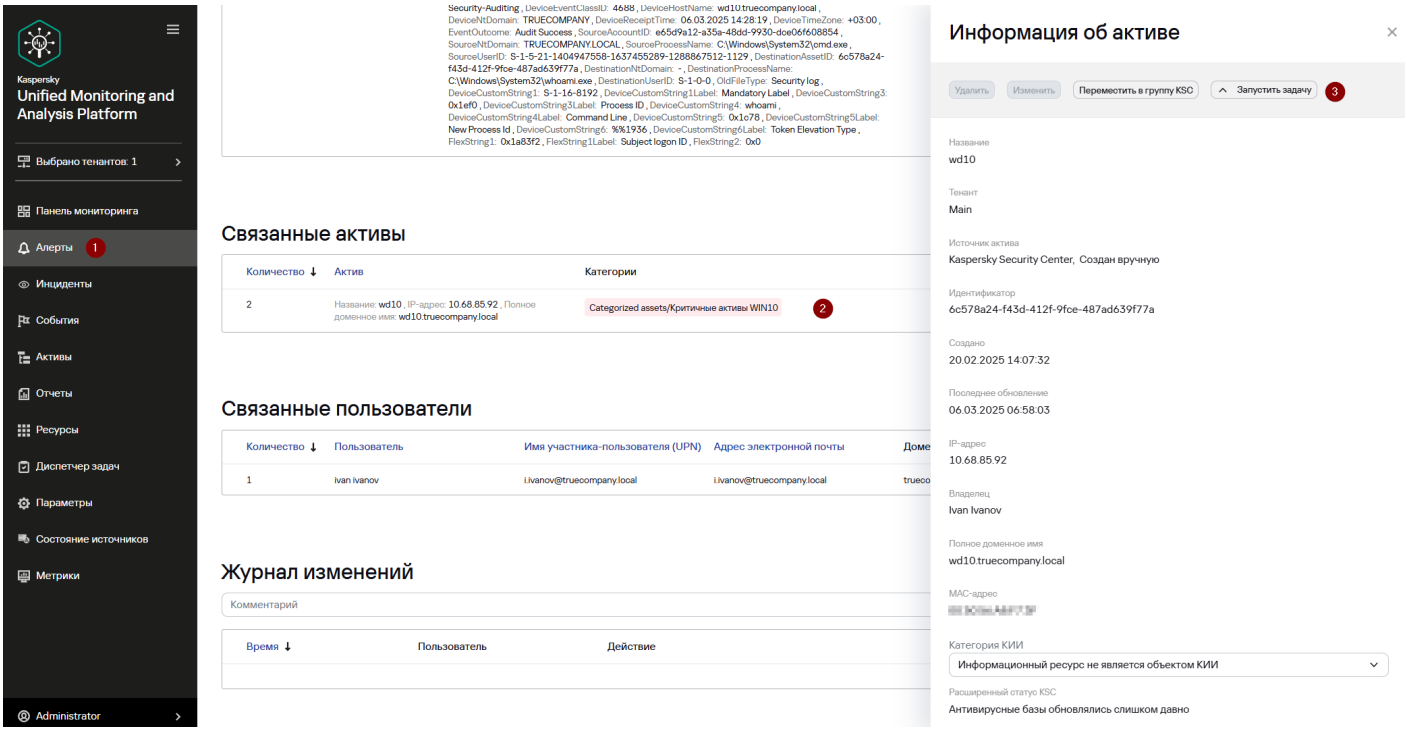
- ??????? **Сохранить**.

?????? ?????????? ???????????? ??? ? ??????? ???????.

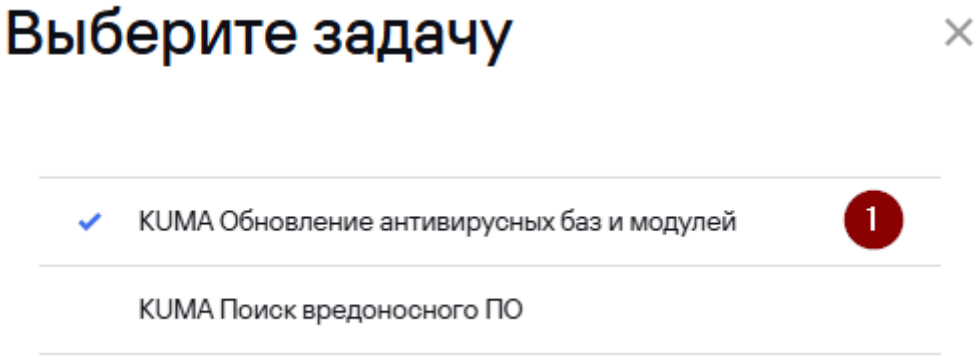
Реагирование вручную средствами Kaspersky Security Center

????? ????????? ???????????? ?????????? Kaspersky Security Center ???????:

- ????????? ? **Алерты** ? ???????? ?????, ? ?????? ???????? ?????????? ????????? ???????? ?? ????????????. ? ????? ??????? ??? ????? **R220_Сбор информации об учетных записях** (??. ?????? ?????? ? ????????)
- ? ???????? ?????? ? ??????? **Связанные активы** ???????? ????? ??? ??????? ?????? .
- ? ??????????? ???? **Информация об активе** ??????? **Запустить задачу**.



- ? ?????????????? ?????? ???????? **Реагирование KSC** ? ????? ????? ????????? ?????? **KUMA Обновление антивирусных баз и модулей** (????? ???????? ?????? KUMA **Поиск вредоносного ПО** ???????? ?????? ?????????? ??? ????????? ???????? ?????????? ???????? ???????????? ??).

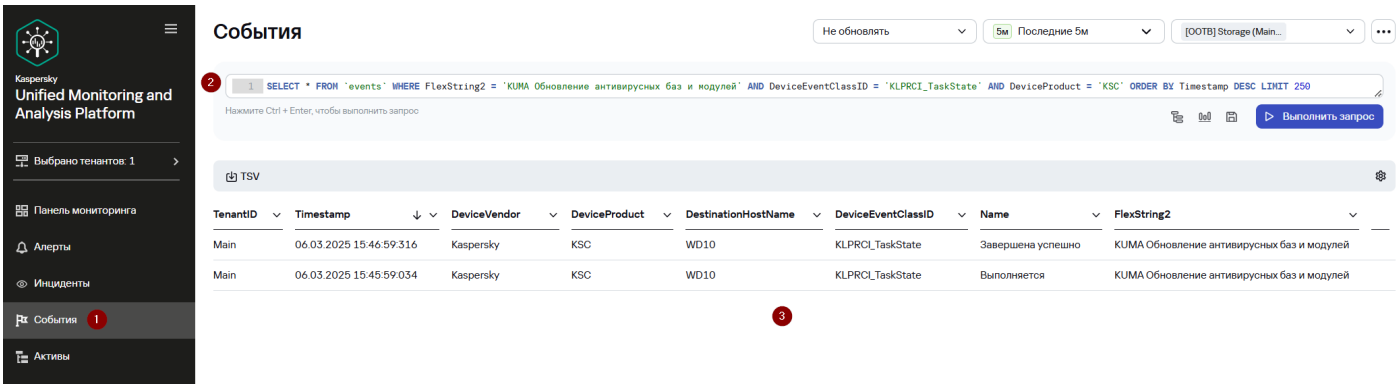


- ??????? **Запустить**.

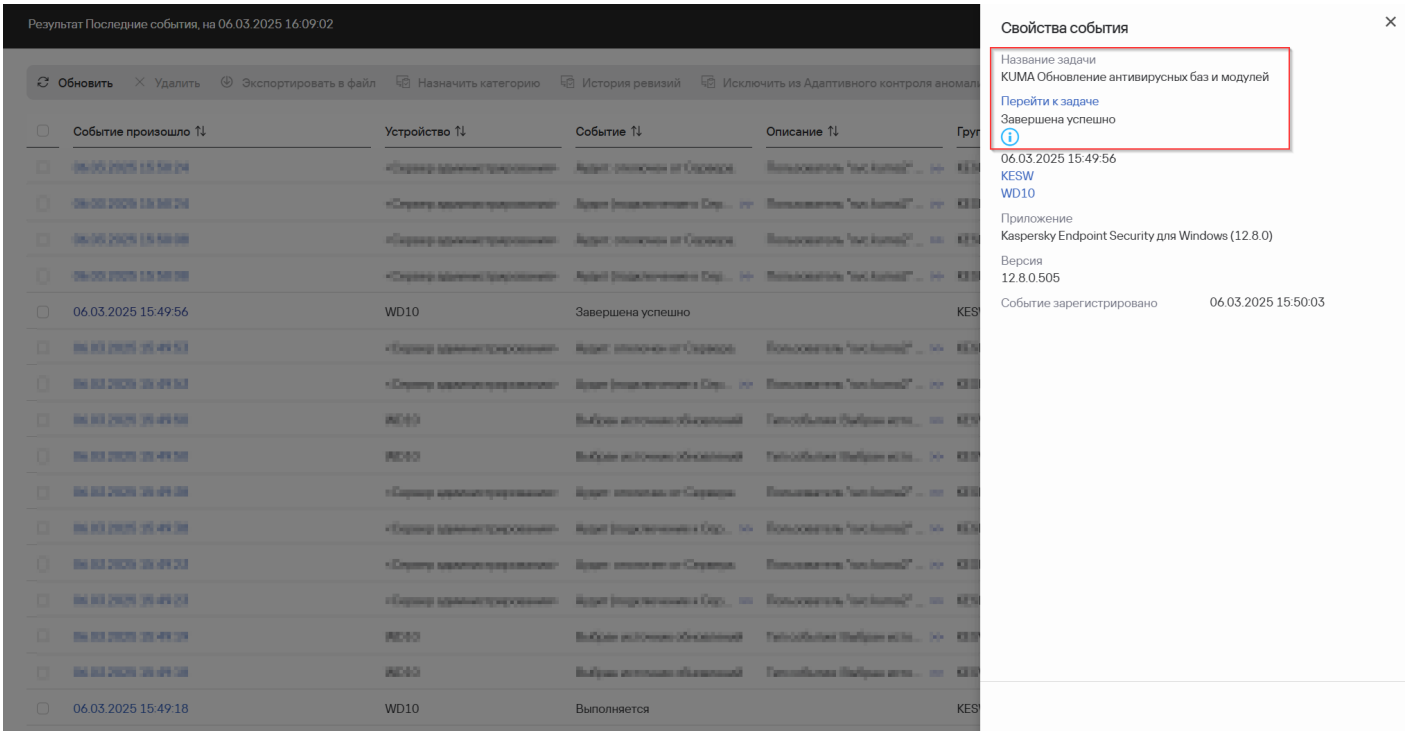
?????? ?????????? ?? ????????? ?????? ????????.

????? ?????????, ??? ?????? ???? ???????? ? ????????? ??????? ????????? ? ?????? **События** ? ????????? ????????? ????????? ??????:

```
SELECT * FROM `events` WHERE FlexString2 = 'KUMA ?????????? ???????????? ??? ? ???????' AND DeviceEventClassID
= 'KLPRCI_TaskState' AND DeviceProduct = 'KSC' ORDER BY Timestamp DESC LIMIT 250
```

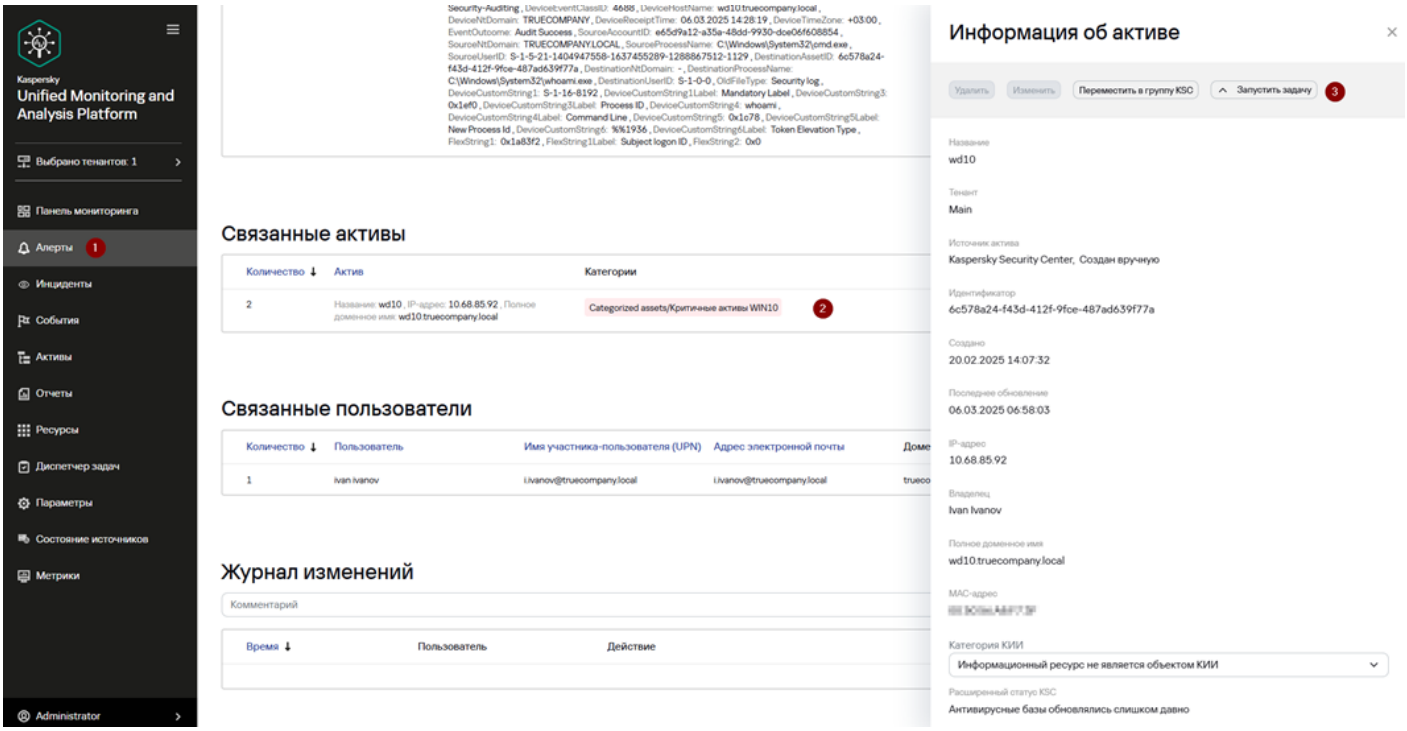


????? ?????? ?????????? ?????? ????? ?????????? ? ??????? Kaspersky Security Center ??? ?????????????? ? ?????????? ?????????? Kaspersky Endpoint Security.

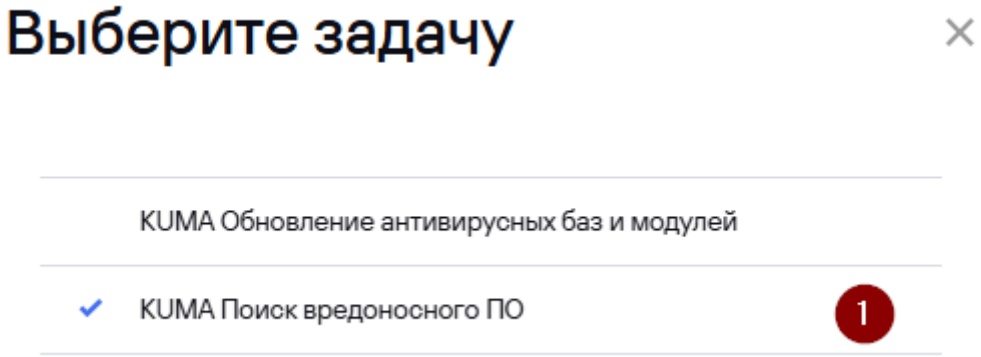


????? ????????? ????? ????????? ?????? KUMA ????? ???????????? ??:

- ????????? ? **Алерты** ? ???????? ?????, ? ?????? ???????? ?????????? ????????? ???????? ?? ????????????. ? ????? ??????? ??? ????? **R220_Сбор информации об учетных записях**.
- ? ???????? ?????? ? ??????? **Связанные активы** ???????? ????? ??? ??????? ?????? .
- ? ??????????? ???? **Информация об активе** ??????? **Запустить задачу**.



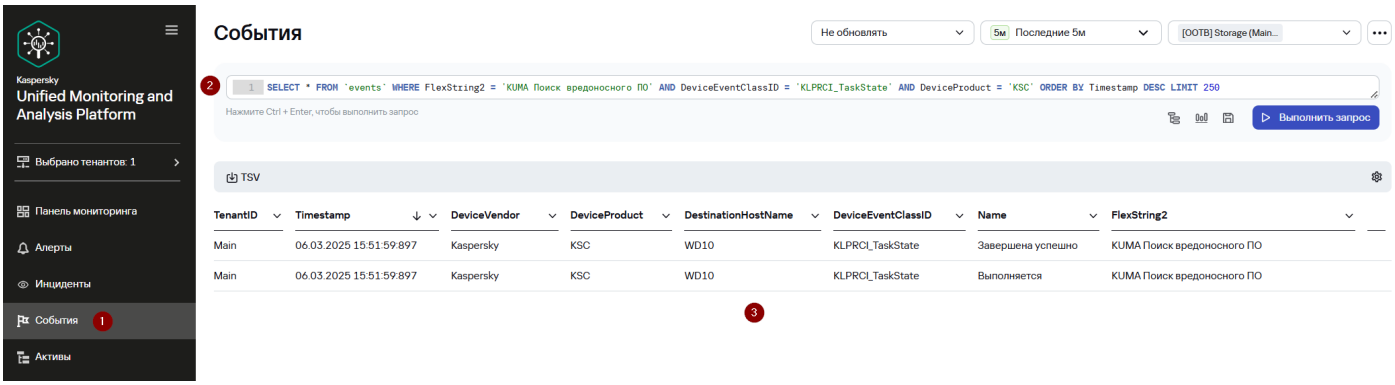
- ? ?????????????? ?????? ???????? **Реагирование KSC** ? ????? ????? ????????? ?????? **KUMA Поиск вредоносного ПО**.
- ??????? **Запустить.**



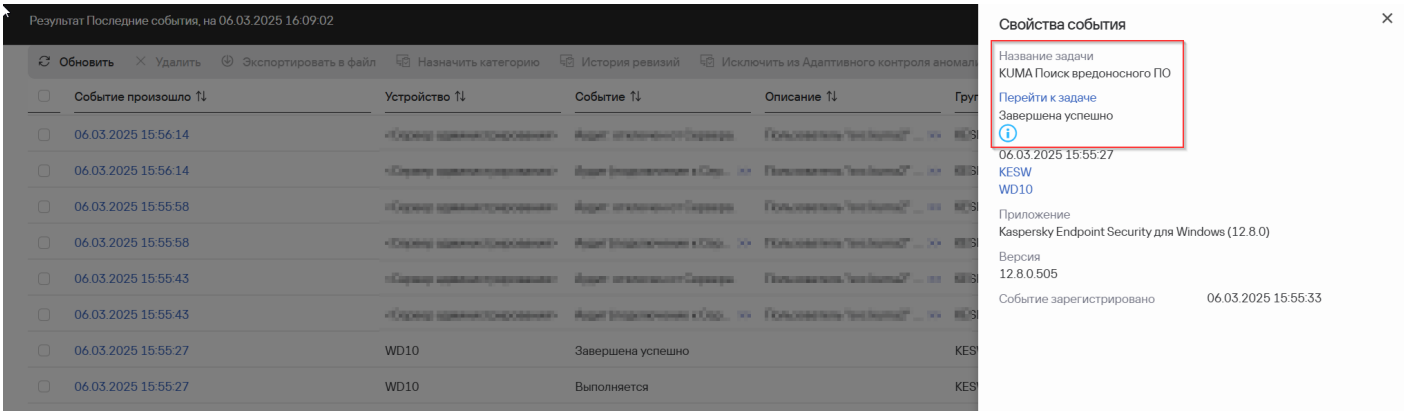
?????? ?????? ???????????? ?? ?? ????????? ?????? ????????.

????? ?????????, ??? ?????? ????????? ??????? ????????? ? ?????? **События** ? ????????? ????????? ????????? ??????:

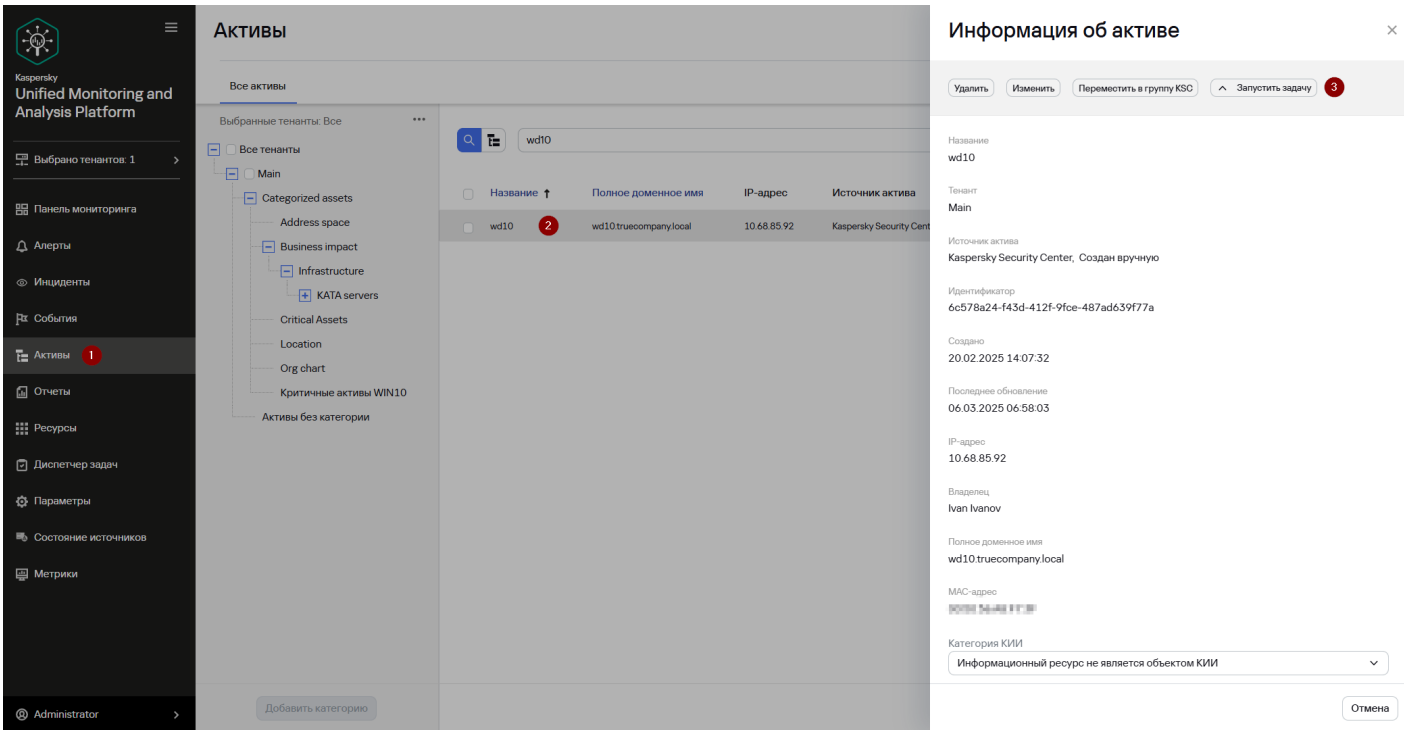
```
SELECT * FROM `events` WHERE FlexString2 = 'KUMA ????? ???????????? ??' AND DeviceEventClassID =
'KLPRCI_TaskState' AND DeviceProduct = 'KSC' ORDER BY Timestamp DESC LIMIT 250
```

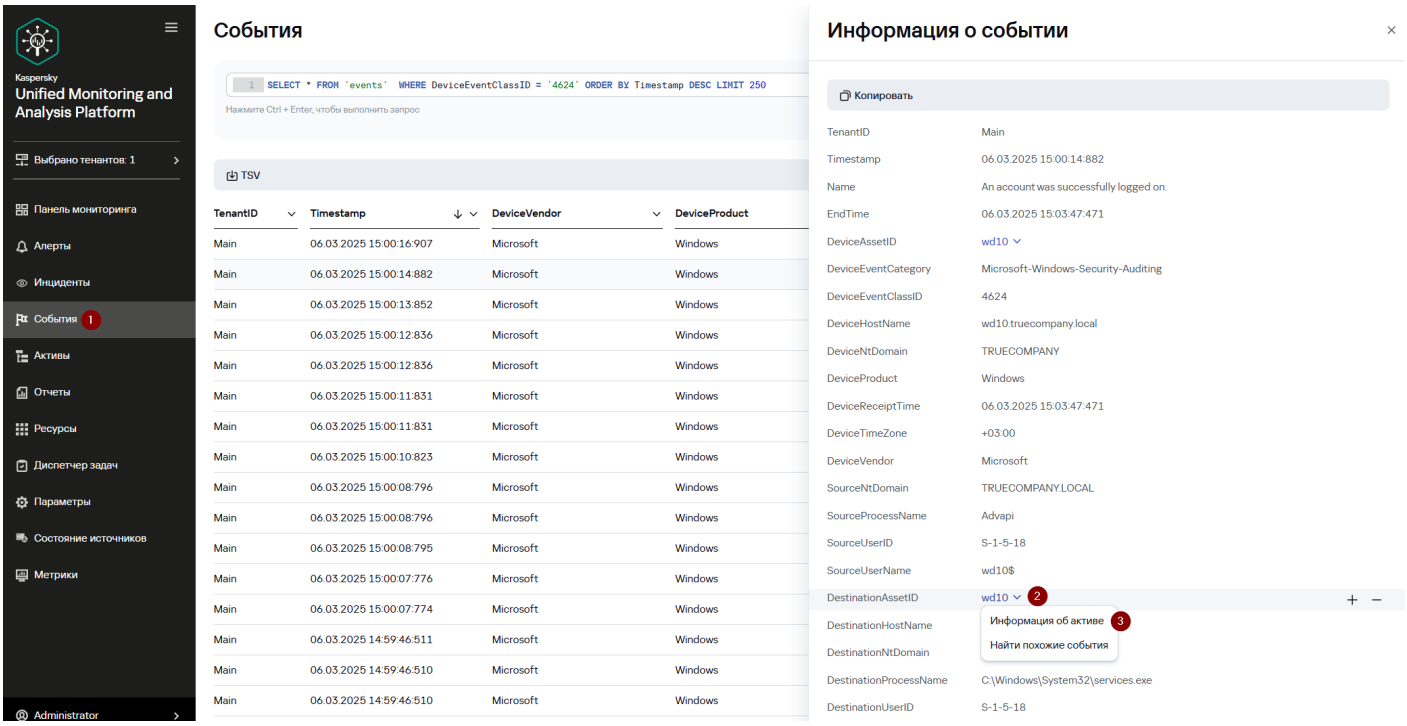


????? ?????? ?????????? ?????? ????? ?????????? ? ??????? Kaspersky Security Center ??? ?????????????? ? ?????????? ?????????? Kaspersky Endpoint Security.



????????? ??????? ???????????? ?????????? Kaspersky Security Center ????? ????? ?? ??????? **Активы**, ?????? ?????????????? ????? ?? ??????, ??? ?? ???????? **События**, ????? ?? ??? ?????? ? ???? ***AssetID**.





?????? ??????-??????? «?????????????? ?????? ????? Kaspersky Security Center»: https://support.kaspersky.ru/kuma/4.0/218008

Revision #3
Created 2026-08-12 11:17:46 UTC by Dmitry Borisov
Updated 2026-08-12 12:56:29 UTC by Dmitry Borisov