Интеграция с Kaspersky Threat Intelligence Portal

> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

> Статья онлайн-справки «Интеграция с Kaspersky Threat Intelligence Portal»: https://support.kaspersky.ru/kuma/4.0/217925

Портал **Kaspersky Threat Intelligence Portal** объединяет все знания Лаборатории Касперского о киберугрозах и их взаимосвязи в единую веб-службу. При интеграции с KUMA портал помогает пользователям KUMA быстрее принимать решения, предоставляя им данные о веб-адресах, доменах, IP-адресах, данных WHOIS / DNS.

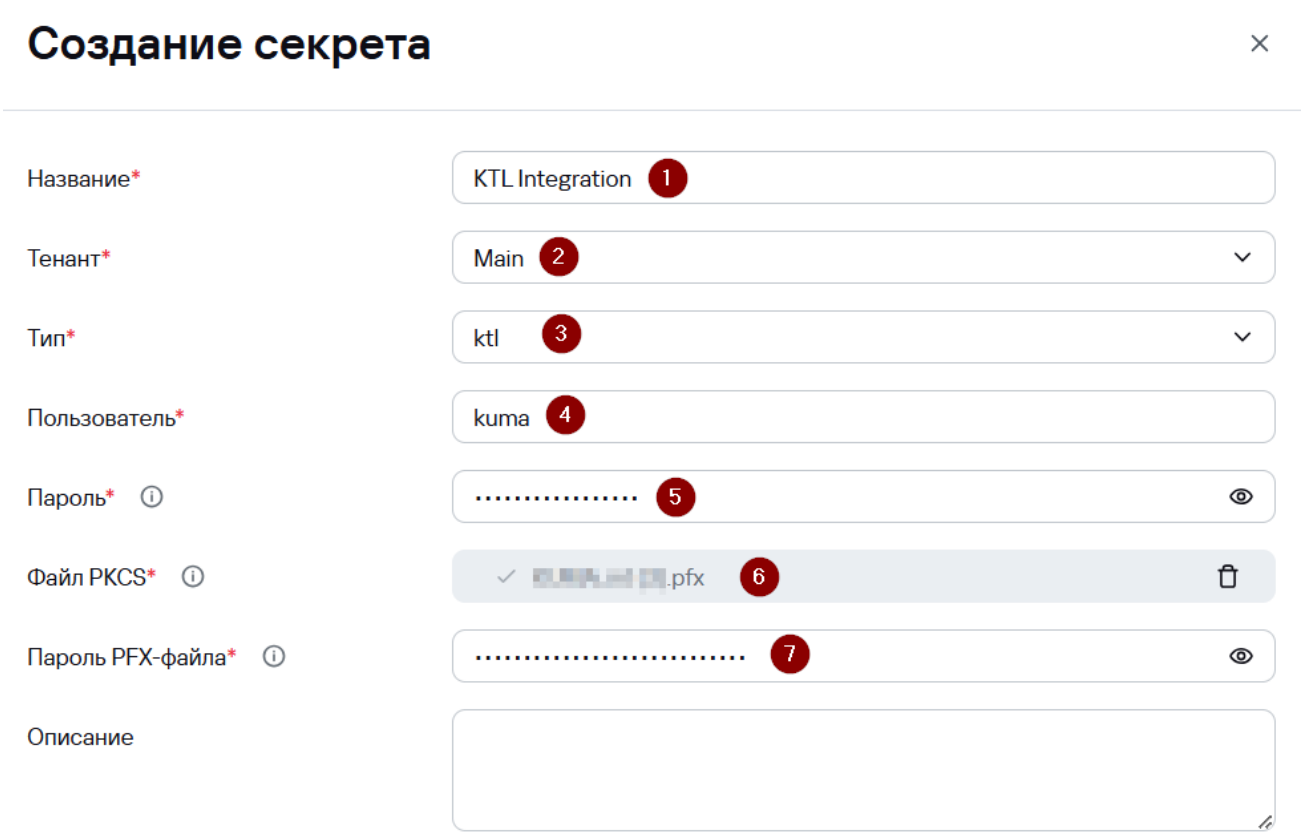
В рамках базовой лицензии KUMA предоставляется доступ к Threat Intelligence Portal. Лицензия KUMA включает в себя возможность сделать до 100 запросов в **Kaspersky Threat Lookup** и до 10 запросов в **Kaspersky Threat Analysis** в период действия лицензии для получения дополнительного контекста в ходе проведения расследований. Чтобы активировать эту функцию, получить дополнительные инструкции и сертификат отправьте запрос с указанием номера заказа на адрес **intelligence@kaspersky.com**.

Создание секрета в KUMA

Предварительно необходимо создать ресурс типа **Секрет** для интеграции с Kaspersky Threat Intelligence Portal:

- Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Секреты**. Отобразится список доступных секретов.
- Нажмите на кнопку **Добавить**, чтобы создать новый секрет. Этот ресурс будет использоваться для хранения данных вашей учетной записи Kaspersky Threat Intelligence Portal.
- В появившемся окне **Создание секрета** введите данные секрета:
  - В поле **Название** укажите имя для добавляемого секрета.
  - В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать создаваемый ресурс.
  - В раскрывающемся списке **Тип** выберите **ktl**.

- В полях **Пользователь** и **Пароль** введите данные своей учетной записи Kaspersky Threat Intelligence Portal (будут предоставлены при запросе на **intelligence@kaspersky.com**).
- Загрузите PFX-файл с учетными данными и сертификатами для доступа к Kaspersky Threat Intelligence Portal (будет предоставлен при запросе на **intelligence@kaspersky.com**):
- Нажмите **Загрузить PFX** и выберите PFX-файл с сертификатом. Имя выбранного файла отображается справа от кнопки Загрузить PFX.
- В поле **Пароль PFX** введите пароль для PFX-файла.
- Нажмите **Создать**.



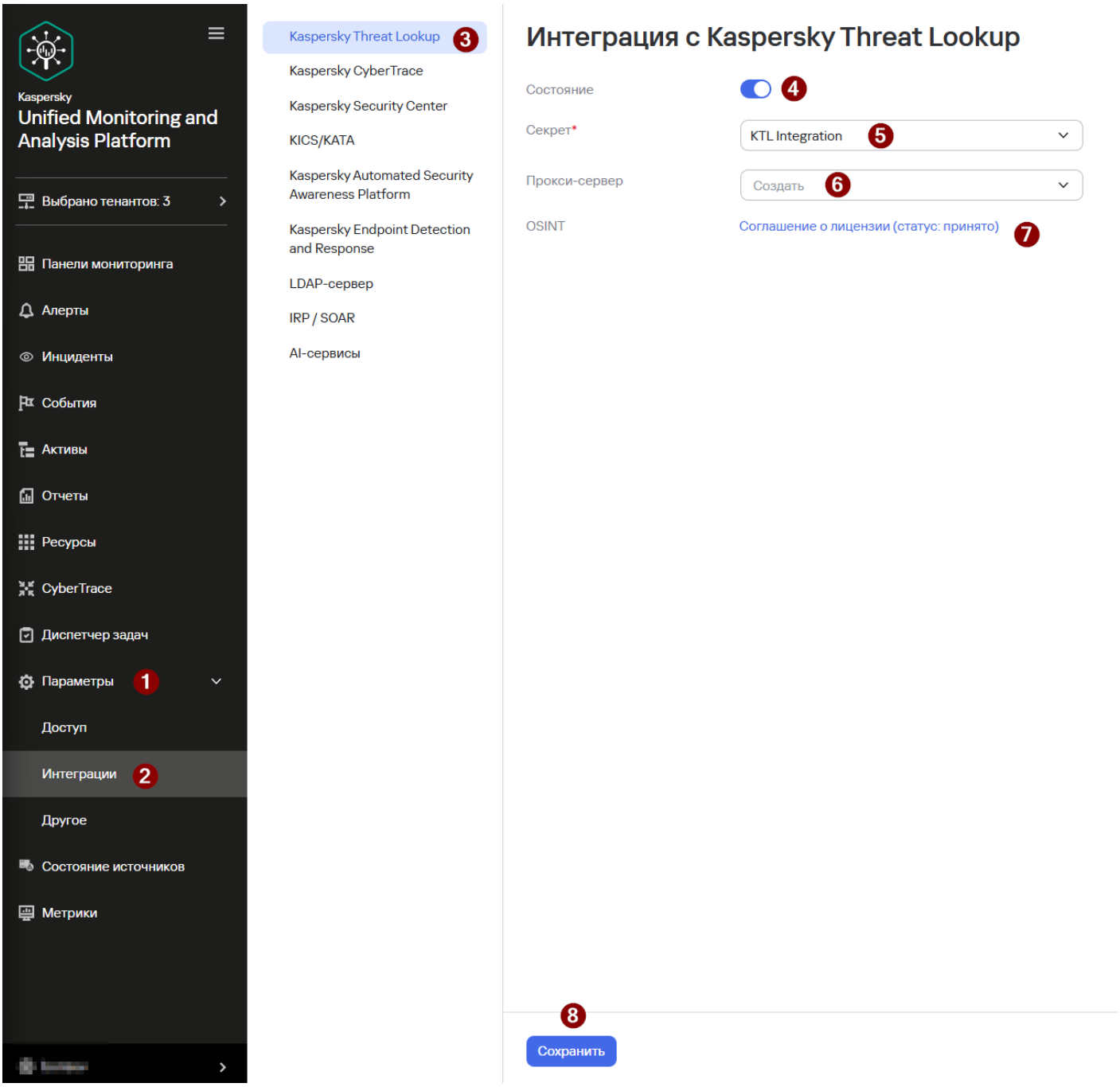
> Из соображений безопасности после сохранения секрета строки, указанные в полях **Пользователь**, **Пароль** и **Пароль для PFX-файла** скрываются

Создание подключения к Kaspersky Threat Lookup

Предварительно выполните вход на портал Kaspersky Threat Intelligence Portal (https://tip.kaspersky.com/), введите данные учетной записи, указанной в ранее созданном секрете, и примите **Условия использования**.

Чтобы создать подключение к Kaspersky Threat Lookup:

- Перейдите в раздел **Параметры** → **Интеграции** → **Kaspersky Threat Lookup** в веб-интерфейсе KUMA.
- Убедитесь, что параметр **Состояние** активен.
- В раскрывающемся списке **Секрет** выберите секрет, который вы создали ранее.
- При необходимости в раскрывающемся списке **Прокси-сервер** выберите прокси-сервер.
- Ознакомьтесь и примите соглашение о лицензии (OSINT)
- Нажмите **Сохранить**.



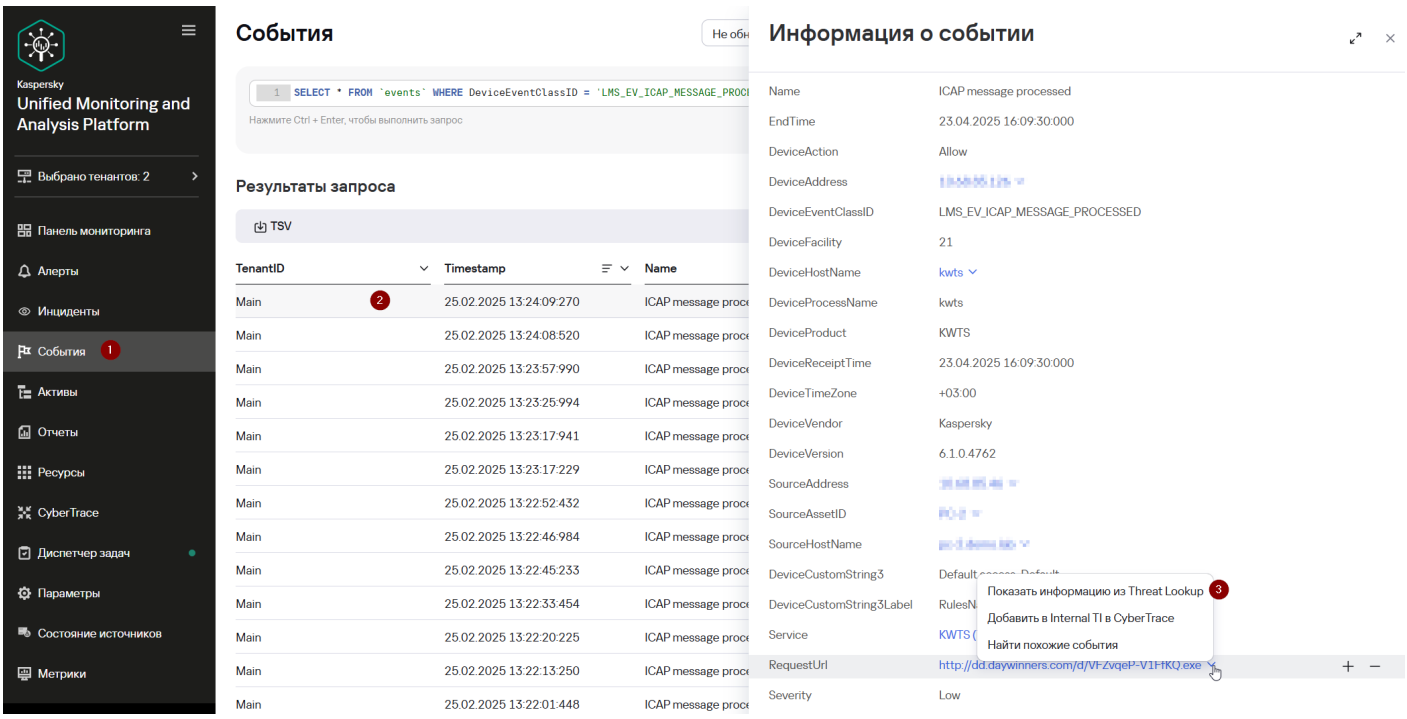
Процесс интеграции KUMA с **Kaspersky Threat Intelligence Portal** завершен.

После интеграции Kaspersky Threat Intelligence Portal и KUMA в области деталей события появится возможность запрашивать сведения о хостах, доменах, URL-адресах, IP-адресах и хешах файлов (MD5, SHA1, SHA256).

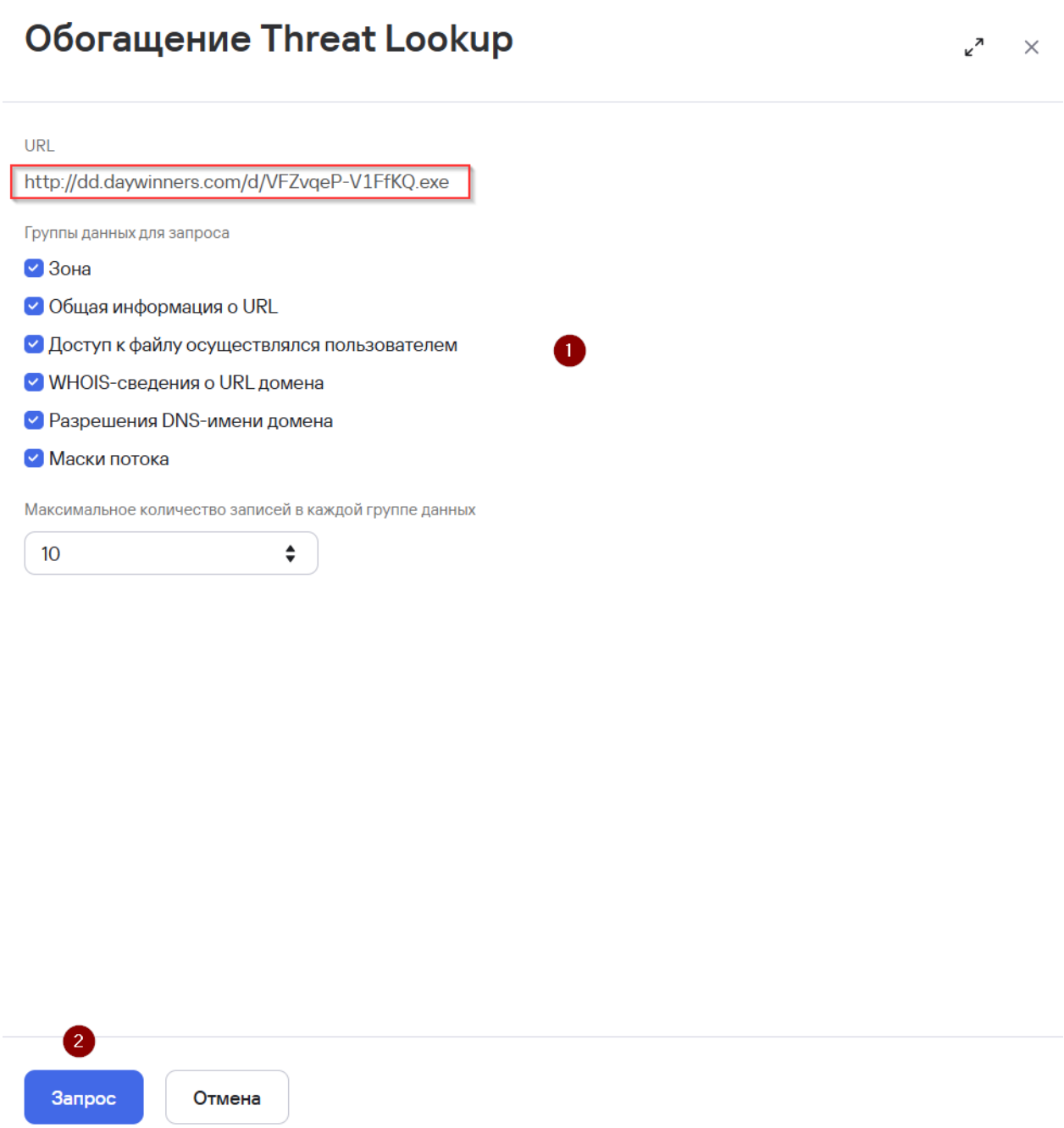
Запрос данных от Kaspersky Threat Intelligence Portal

Чтобы запросить данные от Kaspersky Threat Intelligence Portal:

- Перейдите в раздел **События**, выберите одно из событий в таблице событий.
- В появившемся окне **Информация о событии** нажмите ссылку на домене, URL, IP-адресе или хеш-сумме файла и выберите **Показать информацию из Threat Lookup**.



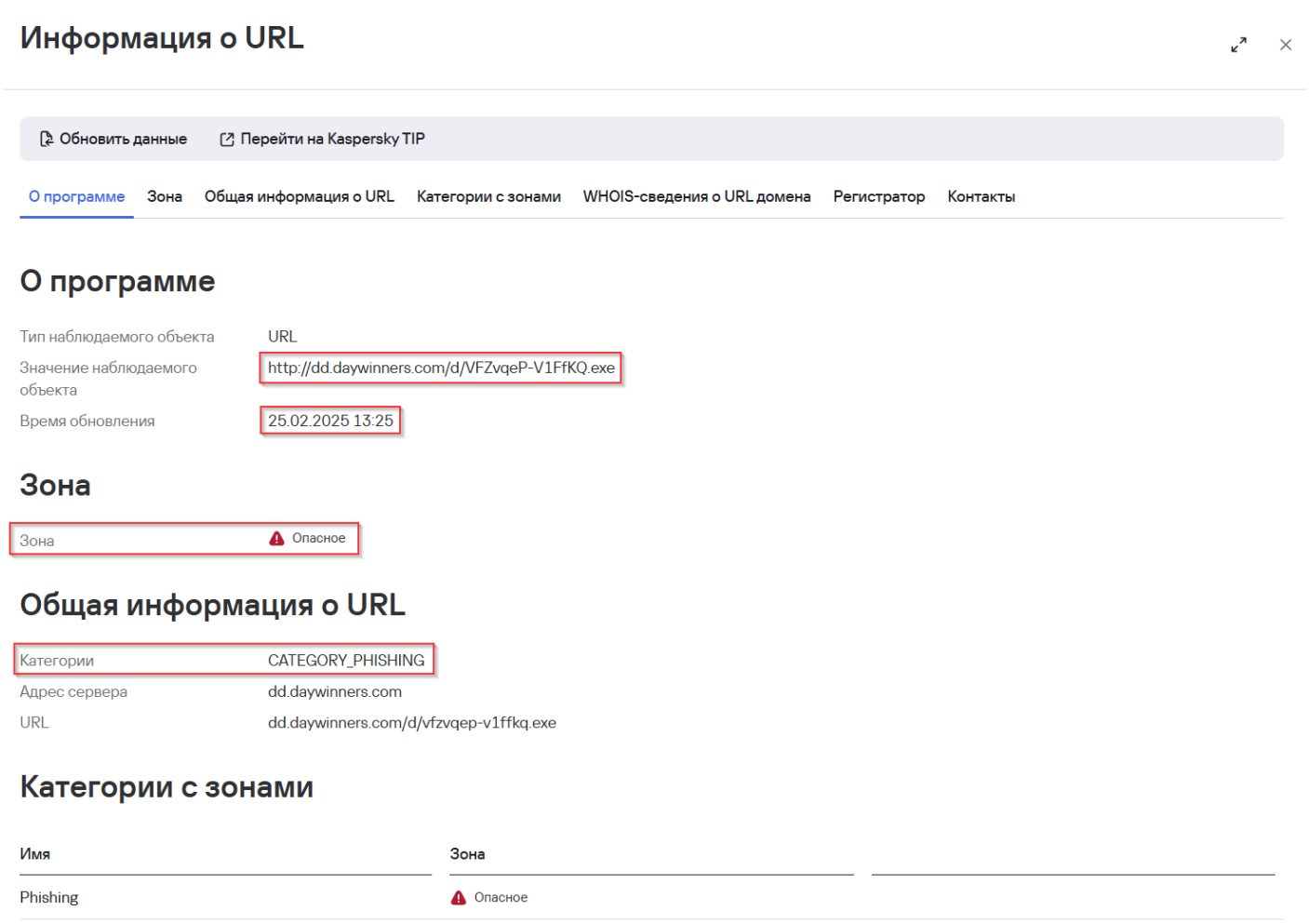
- В окне **Подробнее** нажмите **Обогатить данные Kaspersky TIP**.
- В окне **Обогащение Threat Lookup** выберите группы данных для запроса и нажмите **Запрос**.



Будет создана задача Threat Lookup. После ее завершения события дополнятся данными из Kaspersky Threat Intelligence Portal.

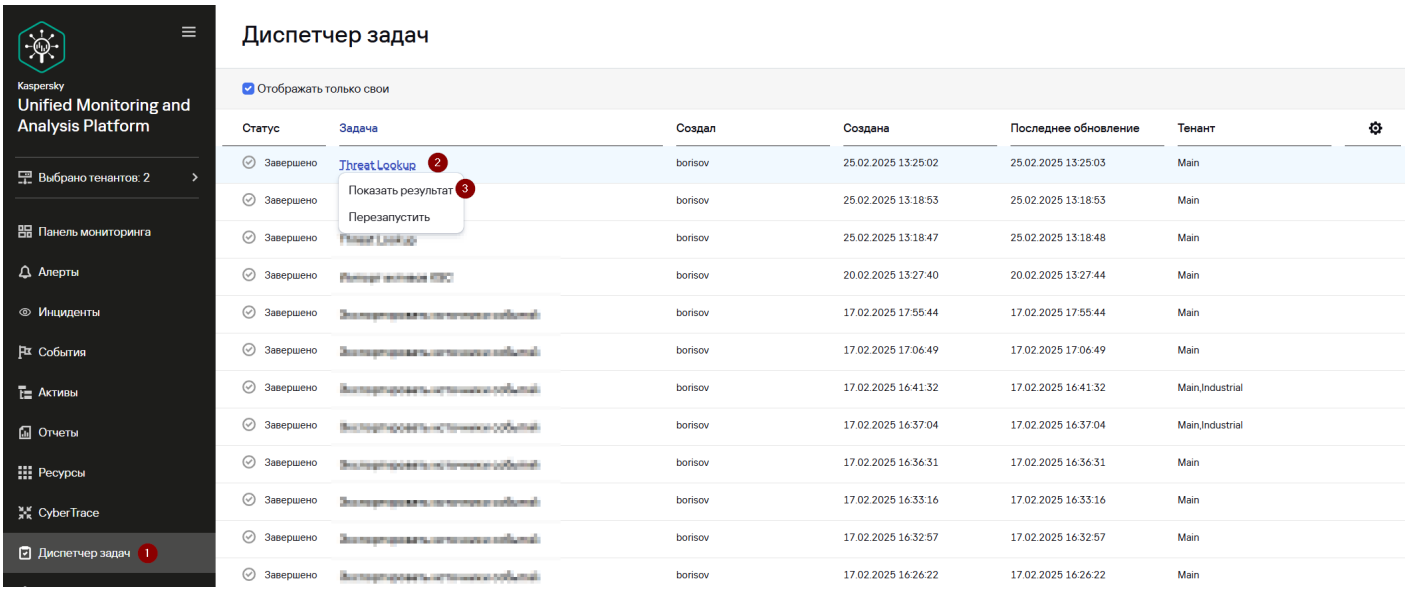
Чтобы просмотреть полученные данные из Kaspersky Threat Intelligence Portal:

- В разделе **События** в окне **Информация о событии** нажмите ссылку на домене, URL, IP-адресе или хеш-сумме файла, для которого вы ранее запрашивали данные от Kaspersky Threat Intelligence Portal, и выберите **Показать информацию из Threat Lookup.**
- В правой части экрана откроется область деталей с данными из Kaspersky Threat Intelligence Portal с указанием времени последнего обновления этих данных.



Информация, полученная от Kaspersky Threat Intelligence Portal, кешируется. Если нажать на домен, веб-адрес, IP-адрес или хеш-файла в области деталей события, для которого у KUMA уже есть доступная информация, вместо окна **Обогащение Threat Lookup** отобразятся данные из Kaspersky Threat Intelligence Portal с указанием времени их получения. Эти данные можно обновить.

Также информацию, полученную от Kaspersky Threat Intelligence Portal, можно посмотреть в **Диспетчере задач**. Для этого перейдите в **Диспетчер задач** выберите задачу **Threat Lookup** и нажмите **Показать результат**.



Revision #7
Created 2026-06-24 14:33:27 UTC by lerat
Updated 2026-08-07 13:14:48 UTC by Dmitry Borisov