

# ???????????? ? Kaspersky TIP

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](mailto:intelligence@kaspersky.com).

## ????????? ??????? ? KUMA

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

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Секреты**. Отобразится список доступных секретов.
2. Нажмите на кнопку **Добавить**, чтобы создать новый секрет. Этот ресурс будет использоваться для хранения данных вашей учетной записи Kaspersky Threat Intelligence Portal.
3. 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 **kti**.
  - В полях **Пользователь** и **Пароль** введите данные своей учетной записи Kaspersky Threat Intelligence Portal (будут предоставлены при запросе на [intelligence@kaspersky.com](mailto: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](mailto: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**.

## Создание секрета

×

|                     |  |
|---------------------|--|
| Название*           | <input type="text" value="KTL Integration"/> 1 |
| Тенант*             | <input type="text" value="Main"/> 2            |
| Тип*                | <input type="text" value="kti"/> 3             |
| Пользователь*       | <input type="text" value="kuma"/> 4            |
| Пароль* ⓘ           | <input type="password" value="....."/> 5       |
| Файл PKCS* ⓘ        | <input type="text" value="✓ [файл].pfx"/> 6    |
| Пароль PFX-файла* ⓘ | <input type="password" value="....."/> 7       |
| Описание            | <input type="text"/>                           |

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

## ????????? ?????????????? ? Kaspersky Threat Lookup

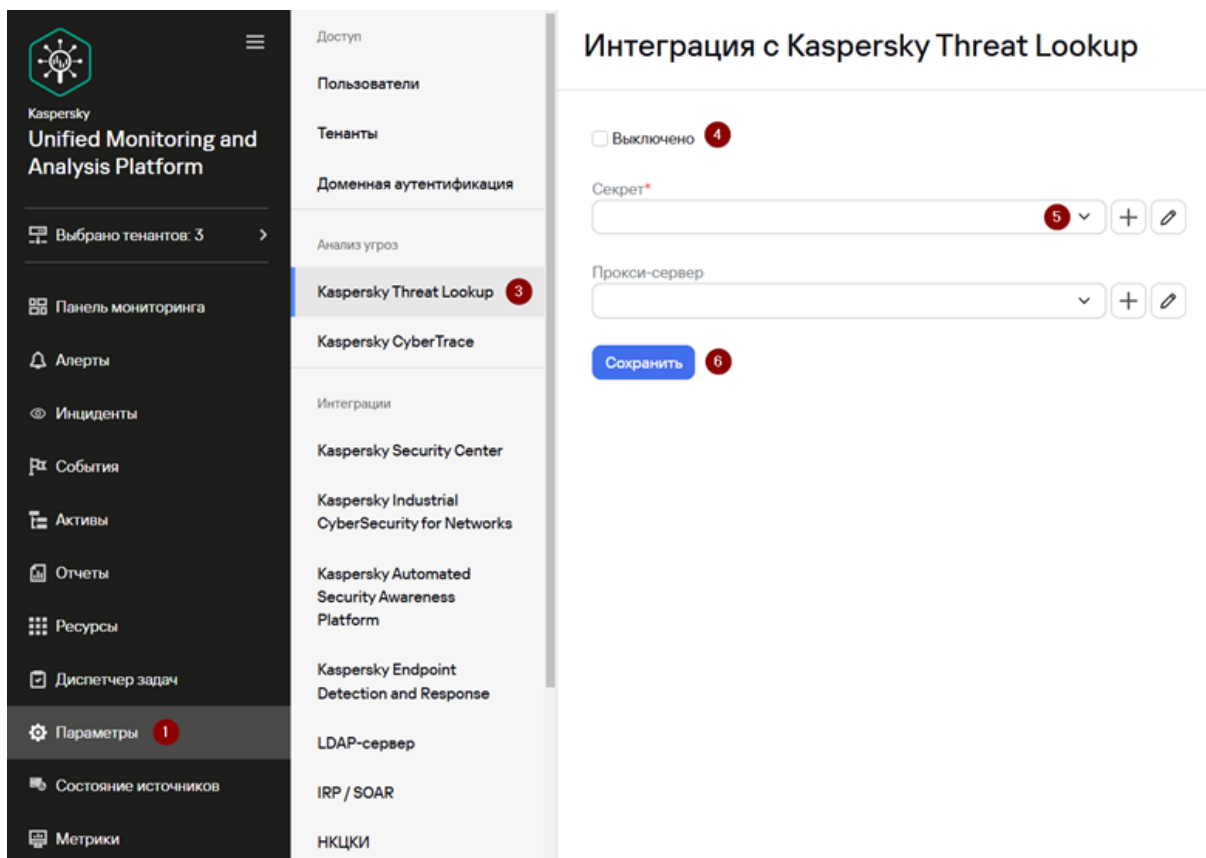
Предварительно выполните вход на портал Kaspersky Threat Intelligence Portal (<https://tip.kaspersky.com/>), введите данные учетной записи, указанной в ранее созданном секрете, и примите **Условия использования**.

Чтобы создать подключение к Kaspersky Threat Lookup:

1. Перейдите в раздел **Параметры** → **Kaspersky Threat Lookup** в веб-интерфейсе КУМА.
2. Убедитесь, что флажок **Выключено** снят.
3. В раскрывающемся списке **Секрет** выберите секрет, который вы создали ранее.

4. При необходимости в раскрывающемся списке **Прокси-сервер** выберите прокси-сервер.

5. 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).

## ?????? ?????? ?? Kaspersky Threat Intelligence Portal

Чтобы запросить данные от Kaspersky Threat Intelligence Portal:

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

3. В окне **Подробнее** нажмите **Обогатить данные Kaspersky TIP**.

4. В окне **Обогащение Threat Lookup** выберите группы данных для запроса и нажмите **Запрос**.

Будет создана задача Threat Lookup. По ее завершении события дополнятся данными из Kaspersky Threat Intelligence Portal.

Чтобы просмотреть полученные данные из Kaspersky Threat Intelligence Portal:

1. 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**.
2. В правой части экрана откроется область деталей с данными из Kaspersky Threat Intelligence Portal с указанием времени последнего обновления этих данных.

## Информация о URL



Обновить данные    Перейти на Kaspersky TIP

[О программе](#)   [Зона](#)   [Общая информация о URL](#)   [Категории с зонами](#)   [WHOIS-сведения о URL домена](#)   [Регистратор](#)   [Контакты](#)

### О программе

|                               |   |
|-------------------------------|---|
| Тип наблюдаемого объекта      | URL   |
| Значение наблюдаемого объекта | <a href="http://dd.daywinners.com/d/VFZvqeP-V1ffkQ.exe">http://dd.daywinners.com/d/VFZvqeP-V1ffkQ.exe</a> |
| Время обновления              | 25.02.2025 13:25  |

### Зона

Зона ⚠ Опасное

### Общая информация о URL


|               |  |
|---------------|--|
| Категории     | CATEGORY_PHISHING                      |
| Адрес сервера | dd.daywinners.com                      |
| URL           | dd.daywinners.com/d/vfzvqep-v1ffkq.exe |

### Категории с зонами

| Имя      | Зона                                       |
|----------|--|
| Phishing | <span style="color: red;">⚠ Опасное</span> |

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**.


  
 Kaspersky
   
 Unified Monitoring and
   
 Analysis Platform

- Выбрано тенантов: 2
- Панель мониторинга
- Алерты
- Инциденты
- События
- Активы
- Отчеты
- Ресурсы
- SubnetTrace
- Диспетчер задач 1

## Диспетчер задач

Отображать только свои

| Статус    | Задача   | Создал  | Создана             | Последнее обновление | Тенант          |  |
|-----------|--|---------|---------------------|----------------------|-----------------|--|
| Завершено | ThreatLookUp <span style="color: red; font-weight: bold;">2</span>       | borisov | 25.02.2025 13:25:02 | 25.02.2025 13:25:03  | Main            |  |
| Завершено | Показать результат <span style="color: red; font-weight: bold;">3</span> | borisov | 25.02.2025 13:18:53 | 25.02.2025 13:18:53  | Main            |  |
| Завершено | Перезапустить  | borisov | 25.02.2025 13:18:47 | 25.02.2025 13:18:48  | Main            |  |
| Завершено | Фильтр событий   | borisov | 20.02.2025 13:27:40 | 20.02.2025 13:27:44  | Main            |  |
| Завершено | Интерпретировать системные события                                       | borisov | 17.02.2025 17:55:44 | 17.02.2025 17:55:44  | Main            |  |
| Завершено | Интерпретировать системные события                                       | borisov | 17.02.2025 17:06:49 | 17.02.2025 17:06:49  | Main            |  |
| Завершено | Интерпретировать системные события                                       | borisov | 17.02.2025 16:41:32 | 17.02.2025 16:41:32  | Main,Industrial |  |
| Завершено | Интерпретировать системные события                                       | borisov | 17.02.2025 16:37:04 | 17.02.2025 16:37:04  | Main,Industrial |  |
| Завершено | Интерпретировать системные события                                       | borisov | 17.02.2025 16:36:31 | 17.02.2025 16:36:31  | Main            |  |
| Завершено | Интерпретировать системные события                                       | borisov | 17.02.2025 16:33:16 | 17.02.2025 16:33:16  | Main            |  |
| Завершено | Интерпретировать системные события                                       | borisov | 17.02.2025 16:32:57 | 17.02.2025 16:32:57  | Main            |  |
| Завершено | Интерпретировать системные события                                       | borisov | 17.02.2025 16:26:22 | 17.02.2025 16:26:22  | Main            |  |

Статья онлайн-справки «Интеграция с Kaspersky Threat Intelligence Portal»:

<https://support.kaspersky.ru/kuma/3.4/217925>

Revision #3

Created 2026-06-24 14:33:27 UTC by lerat

Updated 2026-06-24 14:38:41 UTC by lerat