

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 **kti**.

- 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**.

Создание секрета

×

Название*	KTL Integration 1
Тенант*	Main 2
Тип*	kti 3
Пользователь*	kuma 4
Пароль* ⓘ	 5
Файл PKCS* ⓘ	✓ [файл].pfx 6
Пароль PFX-файла* ⓘ	 7
Описание	

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**.

Kaspersky Unified Monitoring and Analysis Platform

Выбрано тенантов: 3

Панели мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

CyberTrace

Диспетчер задач

Параметры 1

Доступ

Интеграции 2

Другое

Состояние источников

Метрики

Интеграция с Kaspersky Threat Lookup

Состояние 4

Секрет* 5

Прокси-сервер 6

OSINT

Соглашение о лицензии (статус: принято) 7

Сохранить 8

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**.

The screenshot displays the Kaspersky Unified Monitoring and Analysis Platform interface. On the left is a dark sidebar with navigation options: 'Выбрано тенантов: 2', 'Панель мониторинга', 'Алерты', 'Инциденты', 'События' (highlighted with a red circle 1), 'Активы', 'Отчеты', 'Ресурсы', 'CyberTrace', 'Диспетчер задач', 'Параметры', 'Состояние источников', and 'Метрики'. The main area is divided into two panels. The left panel, titled 'События', contains a query builder with a dropdown menu showing 'SELECT', 'FROM', 'events', 'WHERE', and 'DeviceEventClassID = LMS_EV_ICAP_MESSAGE_PROCESSED'. Below the query builder is a table of search results with columns 'TenantID', 'Timestamp', and 'Name'. The table shows multiple rows of events, with the first row highlighted and a red circle 2 next to its 'Timestamp' column. The right panel, titled 'Информация о событии', displays detailed information about the selected event. It includes fields such as 'Name', 'EndTime', 'DeviceAction', 'DeviceAddress', 'DeviceEventClassID', 'DeviceFacility', 'DeviceHostName', 'DeviceProcessName', 'DeviceProduct', 'DeviceReceiptTime', 'DeviceTimeZone', 'DeviceVendor', 'DeviceVersion', 'SourceAddress', 'SourceAssetID', 'SourceHostName', 'DeviceCustomString3', 'DeviceCustomString3Label', 'RulesName', 'Service', 'RequestUrl', and 'Severity'. A red circle 3 highlights the 'RequestUrl' field, which contains the URL 'http://dd.daywinners.com/d/VFZvqetP-V1HKQ.exe'. A dropdown menu is open next to the 'RequestUrl' field, showing options: 'Показать информацию из Threat Lookup' (highlighted with a red circle 3), 'Добавить в Internal TI в CyberTrace', and 'Найти похожие события'.

TenantID	Timestamp	Name
Main	25.02.2025 13:24:09:270	ICAP message processed
Main	25.02.2025 13:24:08:520	ICAP message processed
Main	25.02.2025 13:23:57:990	ICAP message processed
Main	25.02.2025 13:23:25:994	ICAP message processed
Main	25.02.2025 13:23:17:941	ICAP message processed
Main	25.02.2025 13:23:17:229	ICAP message processed
Main	25.02.2025 13:22:52:432	ICAP message processed
Main	25.02.2025 13:22:46:984	ICAP message processed
Main	25.02.2025 13:22:45:233	ICAP message processed
Main	25.02.2025 13:22:33:454	ICAP message processed
Main	25.02.2025 13:22:20:225	ICAP message processed
Main	25.02.2025 13:22:13:250	ICAP message processed
Main	25.02.2025 13:22:01:448	ICAP message processed

Field	Value
Name	ICAP message processed
EndTime	23.04.2025 16:09:30:000
DeviceAction	Allow
DeviceAddress	192.168.1.100
DeviceEventClassID	LMS_EV_ICAP_MESSAGE_PROCESSED
DeviceFacility	21
DeviceHostName	kwts
DeviceProcessName	kwts
DeviceProduct	KWTS
DeviceReceiptTime	23.04.2025 16:09:30:000
DeviceTimeZone	+03:00
DeviceVendor	Kaspersky
DeviceVersion	6.1.0.4762
SourceAddress	192.168.1.100
SourceAssetID	192.168.1.100
SourceHostName	192.168.1.100
DeviceCustomString3	Default
DeviceCustomString3Label	RulesName
Service	KWTS
RequestUrl	http://dd.daywinners.com/d/VFZvqetP-V1HKQ.exe
Severity	Low

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

URL

Группы данных для запроса

- ☒ Зона
- ☒ Общая информация о URL
- ☒ Доступ к файлу осуществлялся пользователем
- ☒ WHOIS-сведения о URL домена
- ☒ Разрешения DNS-имени домена
- ☒ Маски потока

1

Максимальное количество записей в каждой группе данных

2

Запрос

Отмена

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.

🔄 Обновить данные

🔗 Перейти на Kaspersky TIP

О программе

Тип наблюдаемого объекта	URL
Значение наблюдаемого объекта	http://dd.daywinners.com/d/VFZvqeP-V1FfKQ.exe
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	⚠ Опасное

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

CyberTrace

Диспетчер задач1

Диспетчер задач

☒ Отображать только свои

Статус	Задача	Создал	Создана	Последнее обновление	Тенант	
✓ Завершено	ThreatLookup2	borisov	25.02.2025 13:25:02	25.02.2025 13:25:03	Main	
✓ Завершено	Показать результат3	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	ThreatLookup	borisov	25.02.2025 13:18:47	25.02.2025 13:18:48	Main	
✓ Завершено	Результат поиска ИИ	borisov	20.02.2025 13:27:40	20.02.2025 13:27:44	Main	
✓ Завершено	Анализировать активы по ИИ	borisov	17.02.2025 17:55:44	17.02.2025 17:55:44	Main	
✓ Завершено	Анализировать активы по ИИ	borisov	17.02.2025 17:06:49	17.02.2025 17:06:49	Main	
✓ Завершено	Анализировать активы по ИИ	borisov	17.02.2025 16:41:32	17.02.2025 16:41:32	Main,Industrial	
✓ Завершено	Анализировать активы по ИИ	borisov	17.02.2025 16:37:04	17.02.2025 16:37:04	Main,Industrial	
✓ Завершено	Анализировать активы по ИИ	borisov	17.02.2025 16:36:31	17.02.2025 16:36:31	Main	
✓ Завершено	Анализировать активы по ИИ	borisov	17.02.2025 16:33:16	17.02.2025 16:33:16	Main	
✓ Завершено	Анализировать активы по ИИ	borisov	17.02.2025 16:32:57	17.02.2025 16:32:57	Main	
✓ Завершено	Анализировать активы по ИИ	borisov	17.02.2025 16:26:22	17.02.2025 16:26:22	Main	

Revision #7

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

Updated 2026-08-07 13:14:48 UTC by Dmitry Borisov