Events API / API ??? ????????? ???????? ????????? ??????????? ? ???????? ??????????

> Обратите внимание на статью API для получения внешними системами информации о событиях приложения, описывающую процесс создания скрипта, автоматически забирающего события в SIEM/SOAR, как реализацию базового функционала REST API KATA Platform.

Events API / API для получения внешними системами информации о событиях приложения

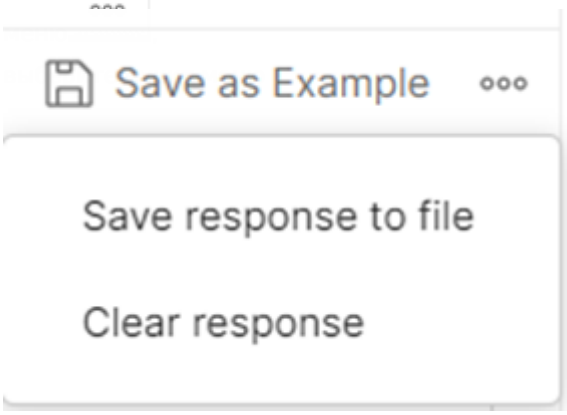
Для создания запроса на вывод информации о событиях используется HTTP-метод GET.
При первом запросе Kaspersky Anti Targeted Attack Platform создает **ContinuationToken** (далее также "токен").
Приложение передает события, доступные в системе на момент создания токена. При создании нового токена Kaspersky Anti Targeted Attack Platform отправляет события, доступные в системе на момент создания этого токена.
Токен содержит информацию о том, какие данные были переданы последними. Если вы хотите получать события, записанные с момента последнего запроса, вам нужно сохранить созданный токен и использовать его в следующих запросах.

Первоначальное получение токена и авторизация рассмотрены в пункте 2.1.

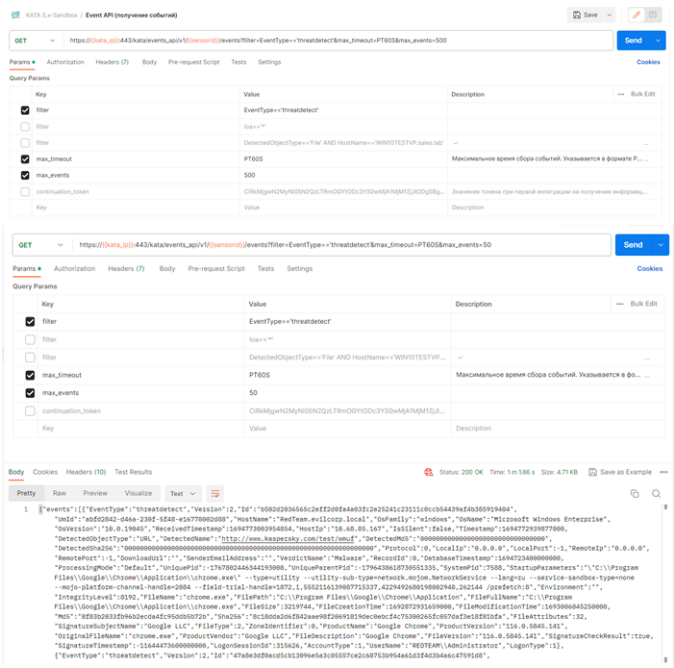
Выберите «**Event API (получение событий)**».
В строке запроса, вы можете добавить параметры filter, max_timeout, max_events, continuation_token.

Нажмите **Send**.
При корректном выводе запроса вы получите статус 200 OK.

Вы можете сохранить информацию об обнаружениях / алертах сохранив вывод в файл. Перейдите в меню вывода информации. Нажмите на значек расширенного



«Save response to file ». Вывод сохранится в виде *.json файла.



Примеры запросов:
GET https://{{kata_ip}}:443/kata/events_api/v1/{{sensorid}}/events?filter=Ioa=='*'&max_timeout=PT300S&max_events=500

GET https://{{kata_ip}}:443/kata/events_api/v1/{{sensorid}}/events?filter=DetectedObjectType=='File' AND HostName=='<FQDN_HostName>'&max_timeout=PT60S&max_events=50

GET "https://{{kata_ip}}:443/kata/events_api/v1/{{sensorid}}/events=?filter=EventType=='threatdetect' AND EventType=='threatprocessingresult'&max_timeout=PT300S&max_events=64000

Синтаксис:
GET "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию 443>/kata/events_api/v1/<идентификатор external_system_id>/events=?filter=<фильтр для событий>&max_timeout=<максимальное время сбора событий>&max_events=<максимальное количество событий>&continuation_token=<значение токена, полученное при первом запросе>"

Если при первом запросе вы указали значение параметра filter, при повторном запросе вы можете его не указывать: параметры фильтрации сохраняются от предыдущего запроса и используются в случае, если не указаны новые. Если вы не хотите использовать фильтрацию, не указывайте значение для параметра.

Запрос на вывод информации о событиях для cURL https://support.kaspersky.com/help/KATA/7.1/ru-RU/248951.htm
Полное описание логики запроса: языка, параметров приведено в Приложении 2 Event API, но для краткости,

Revision #4
Created 16 December 2025 14:25:52 by Владислав
Updated 6 February 2026 11:29:46 by Кирилл