?????????? ??????? ??????? (Postman) ?? API ? Central node KATAP

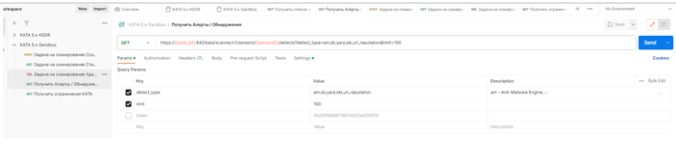
?????????? ??????? ??????? (postman) ?? api ? Central Node kata

Вы можете настроить интеграцию Kaspersky Anti Targeted Attack Platform с внешними системами, чтобы управлять действиями по реагированию на угрозы, а также для проверки хранящихся в них файлов и предоставления внешним системам доступа к информации обо всех обнаружениях и событиях приложения.

Взаимодействие внешних систем с Kaspersky Anti Targeted Attack Platform осуществляется с помощью интерфейса API.

Вызовы методов API доступны только для авторизованных внешних систем.

Для авторизации администратору приложения необходимо создать запрос на интеграцию внешней системы с приложением. После этого администратор должен обработать запрос в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

Создадим запрос на получение обнаружений. Выберите в Postman запрос «Получить Алерты / Обнаружения». Проверьте коректность введенных данных и переменных. На первый запрос, вы получите ответ « **401 Unauthorized**», т.к. Postman (или любая внешняя система) еще не авторизованы.	 https://{{kata_ip}}:443/kata/scanner/v1/sensors/{{sensorid}}/detects?detect_type=am,sb,yara,ids,url_reputation&limit=100 Где: kata_ip – адрес Central Node sensorid – созданный ранее UUID 
Перейдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform. Войдите под УЗ локального администратора. В разделе «**Внешние системы**» отобразится запрос на авторизацию от внешней системы. Нажмите на кнопку **Принять**.	

Внешняя система будет авторизована. Обратите внимание на «ID» и «Отпечаток сертификата». Они должны совпадать с теми данными, которые были введены в Postman (использованы при запросе из сторонней системы)



Выполните повторно запрос «Получить Алерты / Обнаружения».
CN уже выдаст корректный



API для получения внешними системами информации о событиях приложения

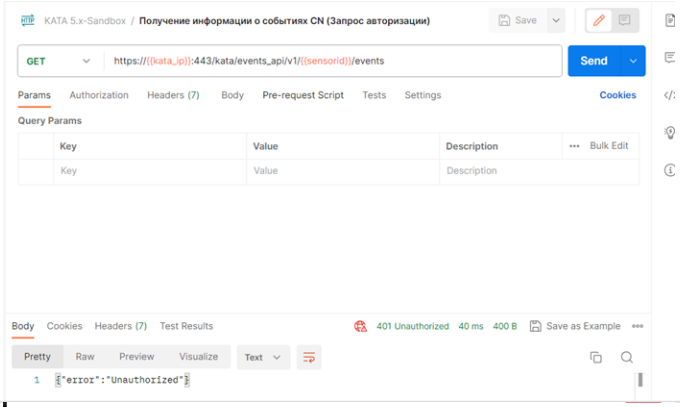
Для получения информации о состоянии приложения и его событиях необходимо дополнительно авторизоваться в системе. (В веб интерфейсе Central Node будет 2 авторизации от внешней системы с одинаковым UUID/IP адресом). Отличие в том, что у вас будет дополнительный токен для авторизации.

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.

Для первого запроса аторизации, запустите команду «Получение информации о событиях CN (Запрос авторизации)»
Будет отправлен запрос на авторизацию в CN.

Пример: GET https://{{kata_ip}}:443/kata/events_api/v1/{{sensorid}}/events



Перейдите в веб-интерфейс Kaspersky Anti Targeted Attack Platform. Войдите под УЗ локального администратора. В разделе «**Внешние системы**» отобразится запрос на авторизацию от внешней системы. Нажмите на кнопку **Принять**.



Внешняя система будет авторизована. Обратите внимание на «ID» и «Отпечаток сертификата». Они должны совпадать с теми данными, которые были введены в Postman (использованы при запросе из сторонней системы)



При повторном запросе, подгрузятся все полседние события на CN, поэтому необходимо выгрузить полученный результат в файл и забрать из него полученный токен.



Revision #7
Created 16 December 2025 07:15:18 by Владислав
Updated 6 February 2026 10:55:44 by Кирилл