??????? ??????? ??????? (POSTMAN) ?? API ? CENTRAL NODE KATA

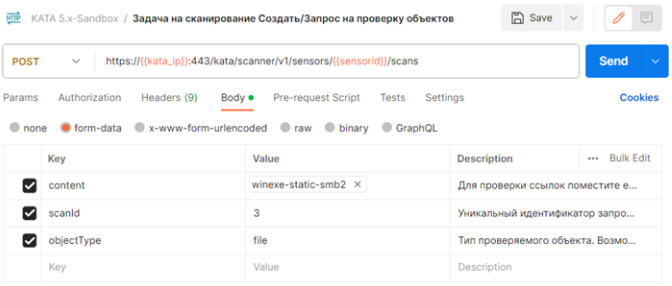
В этом разделе будет рассмотрена коллекция запросов для KATA-KEDR 5.X - 7.1.3 опубликованная в Postman

Убедитесь в корректности настроек переменных и параметров запросов.
Коллекция уже подготовлена.

Обратите внимание, что запросы в Postman несколько отличаются от запросов в cURL! В этом документе рассматриваются запросы на базе Postman, запросы на базе cURL приведены в справке.

Запрос на проверку объектов

Выберите «**Задача на сканирование Создать/Запрос на проверку объектов**».
Откройте **Body – from-data**, выберите файл для отправки на анализ в поле ключа connect. В поле Value будет загружен передаваемый объект.
Нажмите **Send**.



Подробное описание запроса приведено в этой статье справки: https://support.kaspersky.com/help/KATA/7.1/ru-RU/176838.htm

CN KATA вернет ответ 200 OK.

Пример ввода команды с параметрами

curl --cert /root/cert.pem --key /root/server.key -X POST "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans?sensorInstanceId=instance1" -F "content=@/tmp/test" -F scanId=1 -F "objectType=file"

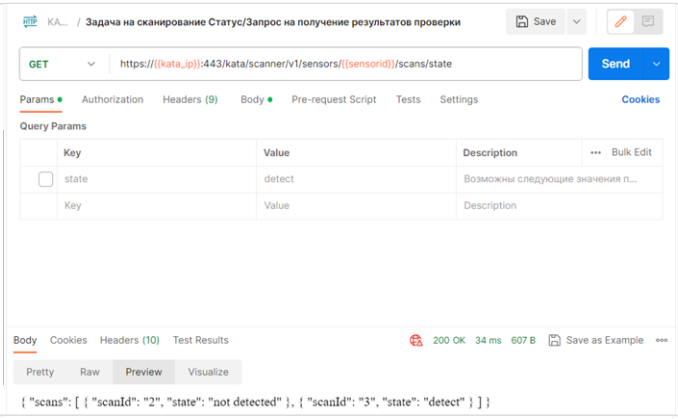
Ограничения

В конфигурационном файле Kaspersky Anti Targeted Attack Platform установлены максимально допустимое количество запросов на проверку объектов от внешних систем и максимально допустимый размер проверяемого объекта.

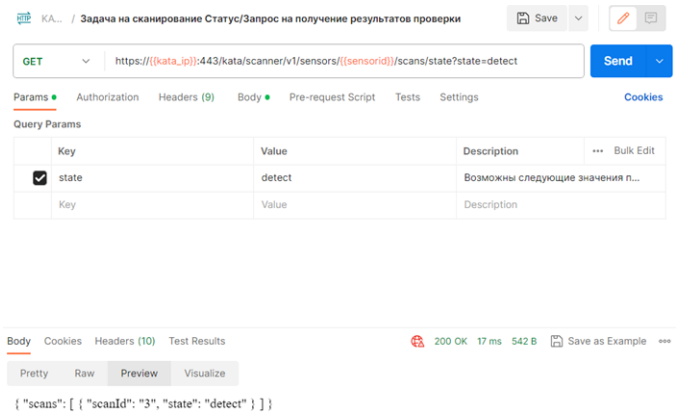
Если превышено максимально допустимое количество одновременных запросов на проверку объектов, Kaspersky Anti Targeted Attack Platform перестает обрабатывать дальнейшие запросы до тех пор, пока количество запросов на проверку объектов не станет меньше максимально допустимого. До этого времени выдается код возврата 429. Необходимо повторить запрос на проверку позже.

Если превышен максимально допустимый размер объекта, Kaspersky Anti Targeted Attack Platform не проверяет этот объект. При создании запроса HTTP-методом POST выдается код возврата 413. Вы можете узнать максимально допустимый размер объекта, просмотрев список ограничений приложения на проверку объектов с помощью метода GET.

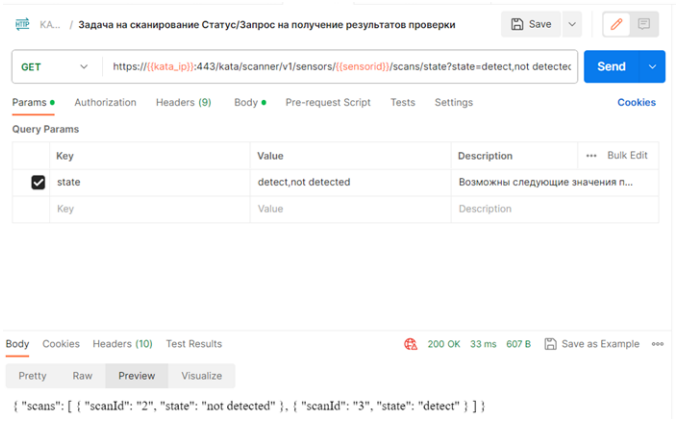
Запрос на получение результатов проверки

Выберите «**Задача на сканирование Статус/Запрос на получение результатов проверки**». Откройте **Params**, Отключите параметр state для вывода всех значений. Нажмите **Send**.	
CN ответит статусом OK 200 с параметрами ответа	

Откройте **Params**, Включите параметр state для вывода всех значений **detect**.
Нажмите **Send**.

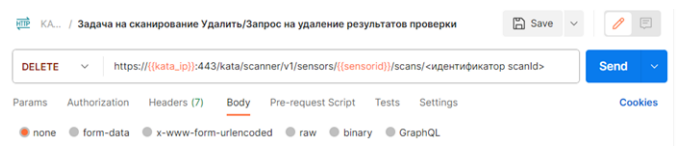


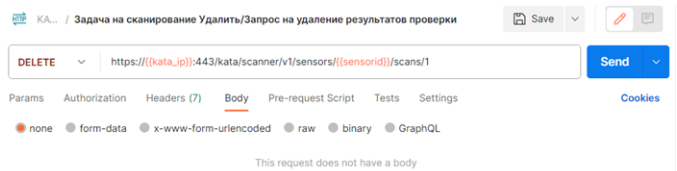
Возможны следующие значения параметра: **detect, not detected, processing, timeout, error**.
Через запятую можно выбирать несколько параметров

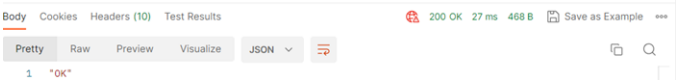


Запрос на удаление результатов проверки

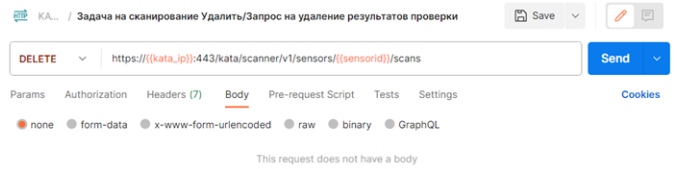
Выберите «**Задача на сканирование Удалить/Запрос на удаление результатов проверки**».
В строке запроса параметр <идентификатор scanId> должен иметь значение номера сканирования из предыдущей задачи скана объектов либо отсутствовать.
Нажмите **Send**.

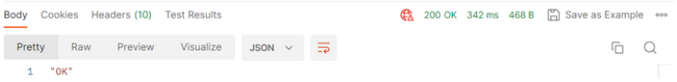




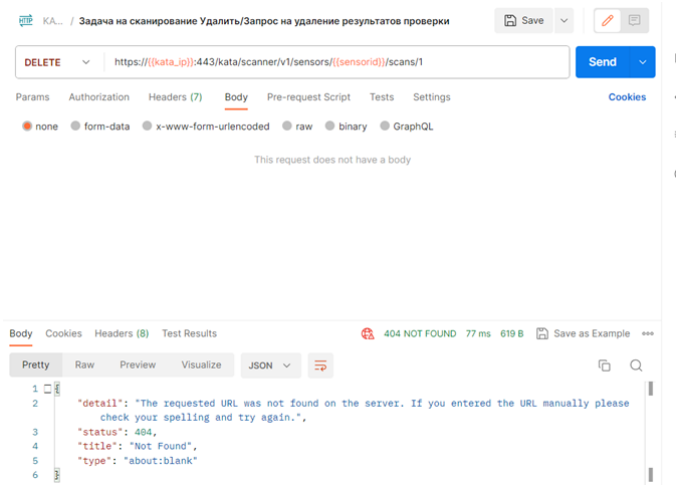


Если этот параметр <идентификатор scanId> не задан, будут удалены результаты проверки всех объектов.



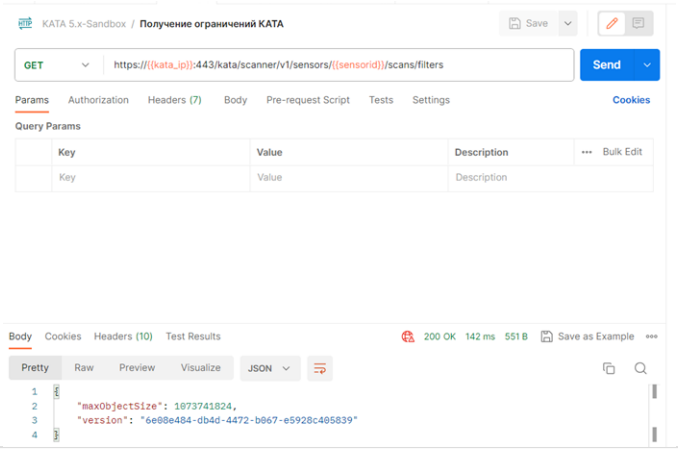


Если <идентификатор scanId> указан не верно, то CN ответит статусом OK 400



Получение ограничений KATA

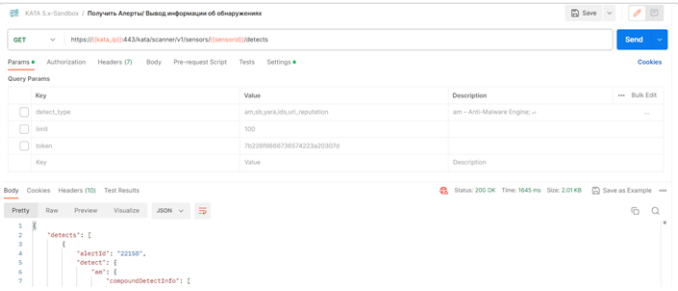
Выберите «**Получение ограничений KATA**».
Нажмите **Send**.
При успешной обработке запроса отобразятся ограничения приложения на проверку объектов.
Ограничение **maxObjectSize** – максимально допустимый размер объекта, который вы можете отправить на проверку.



Запрос на вывод информации об обнаружениях (Получение Алертов)

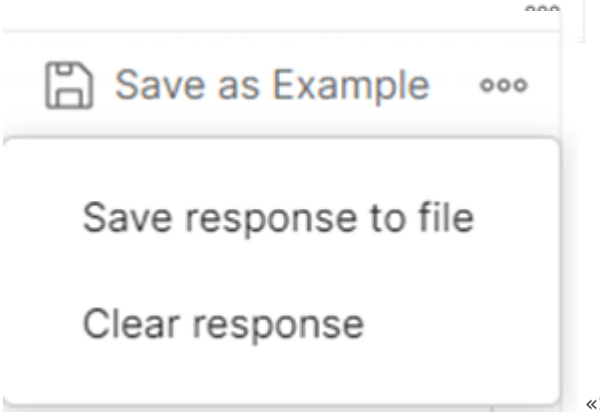
Выберите «**Получить Алерты/ Вывод информации об обнаружениях**».
В строке запроса, вы можете добавить параметры detect_type, limit, token.

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

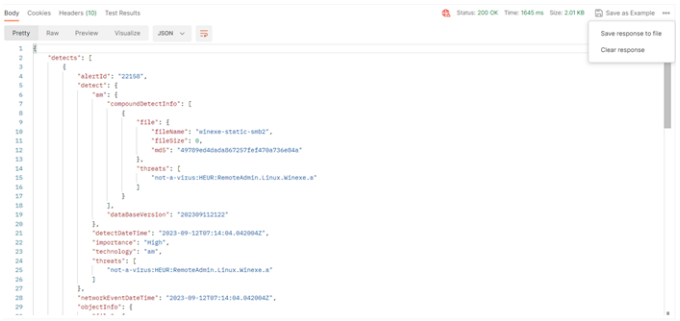


Параметр detect_type описывает технологию, с помощью которой выполнено обнаружение. Возможно указать несколько технологий через запятую.Возможные значения:
am – Anti-Malware Engine;
sb – Sandbox;
yara – YARA;
url_reputation – URL Reputation;
ids – Intrusion Detection System;
Если параметр не указан, предоставляется информация обо всех обнаружениях.

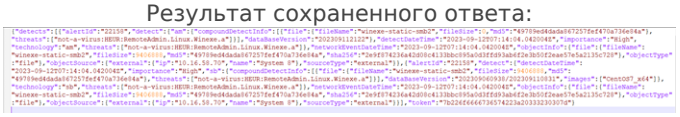
Вы можете сохранить информацию об обнаружениях / алертах сохранив вывод в файл. Перейдите в меню



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



Результат сохраненного ответа:



Состав передаваемых данных обширен, полный перечень всех данных описан в разделе «Состав передаваемых данных» раздела «Взаимодействие с внешними системами по API».
Так же таблица с описанием передаваемых данных приведена в приложении 1.

Revision #6
Created 16 December 2025 14:01:25 by Владислав
Updated 6 February 2026 10:55:44 by Кирилл