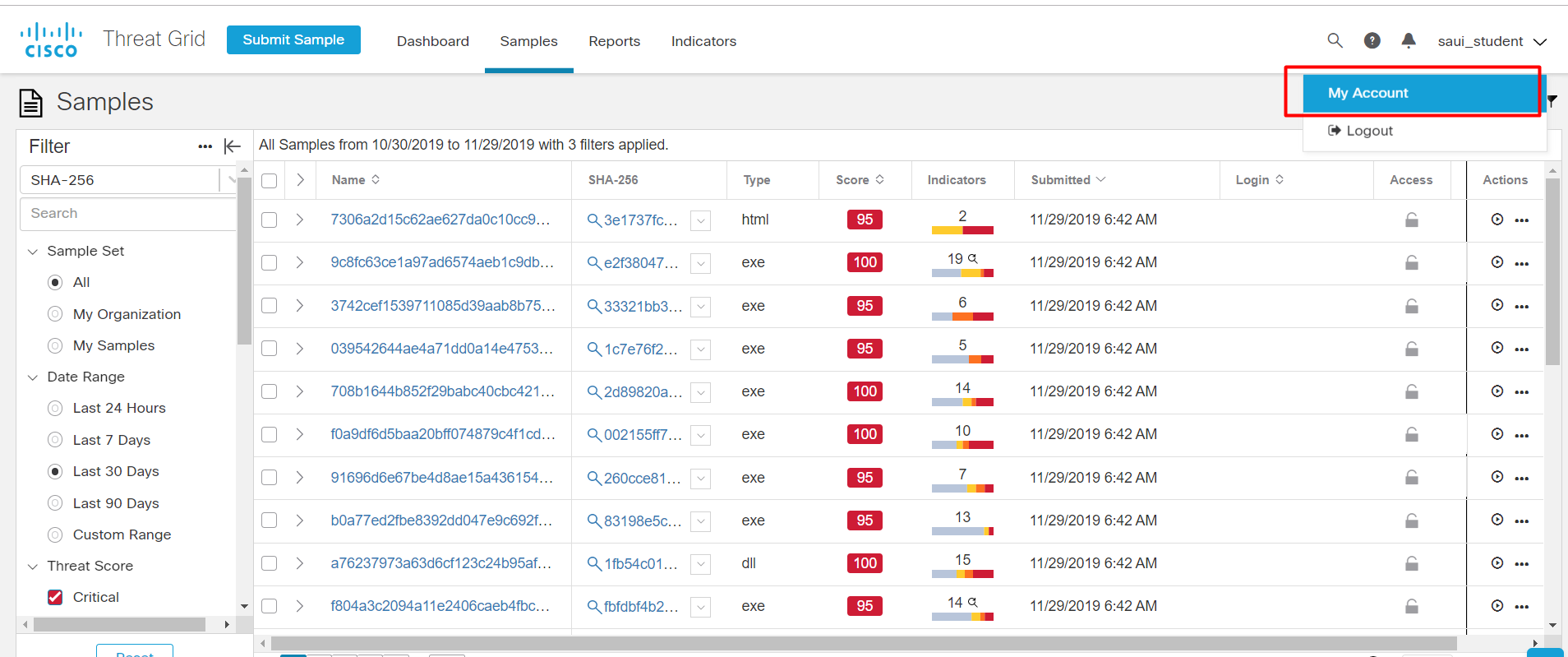
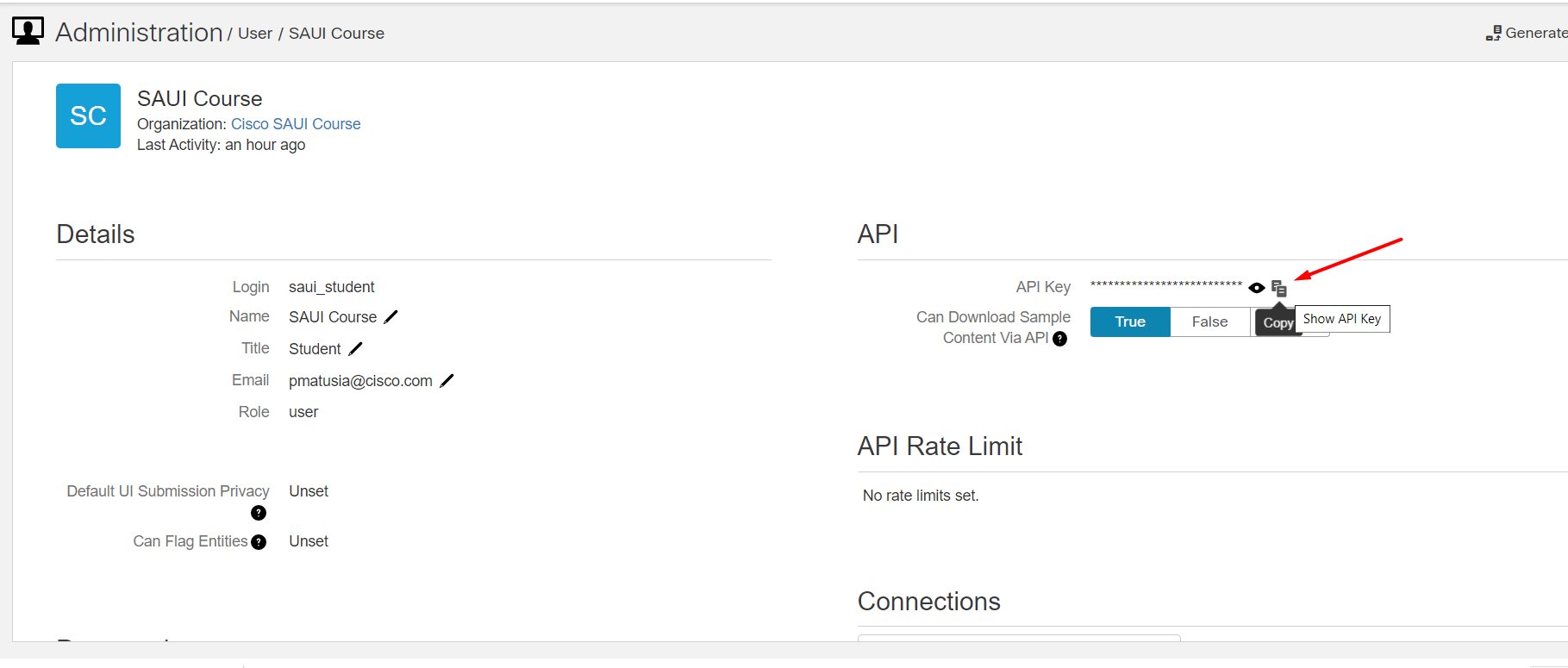
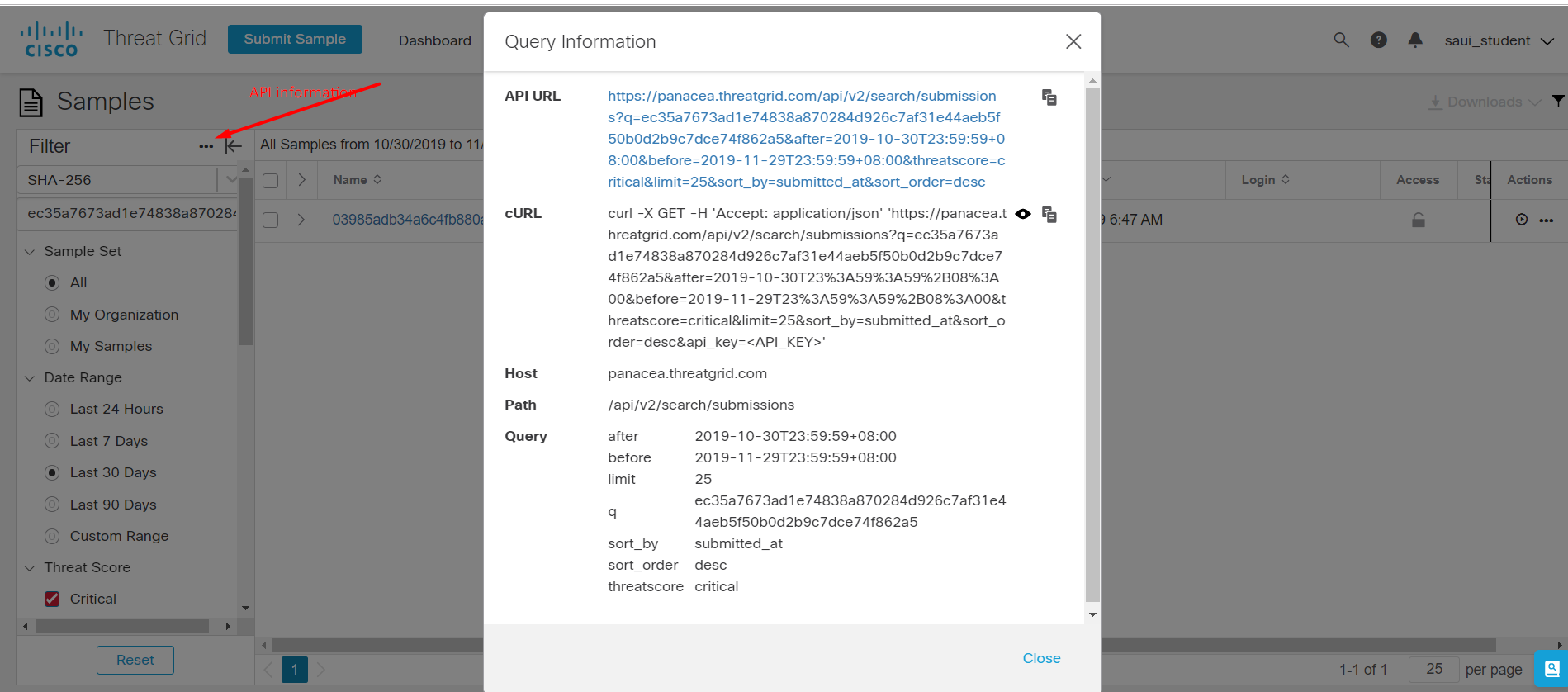
**45) TG - Authenticate to Cisco Threat Grid API**

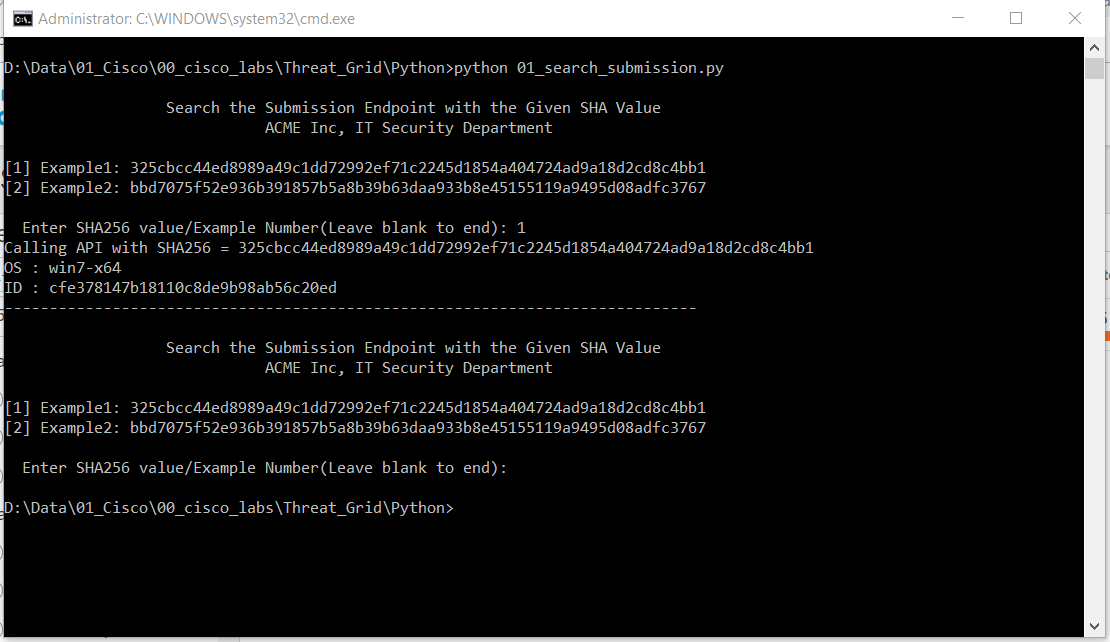




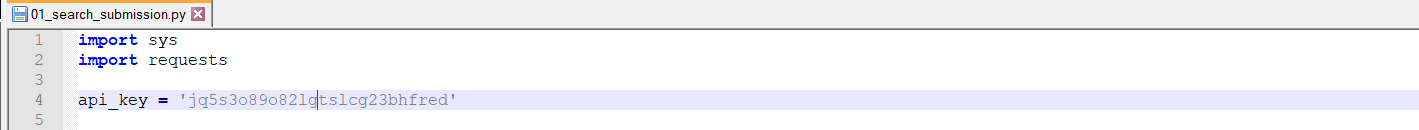
**46) TG - Search the Submissions Endpoint with the Given SHA Value**

<https://panacea.threatgrid.com/mask/samples>



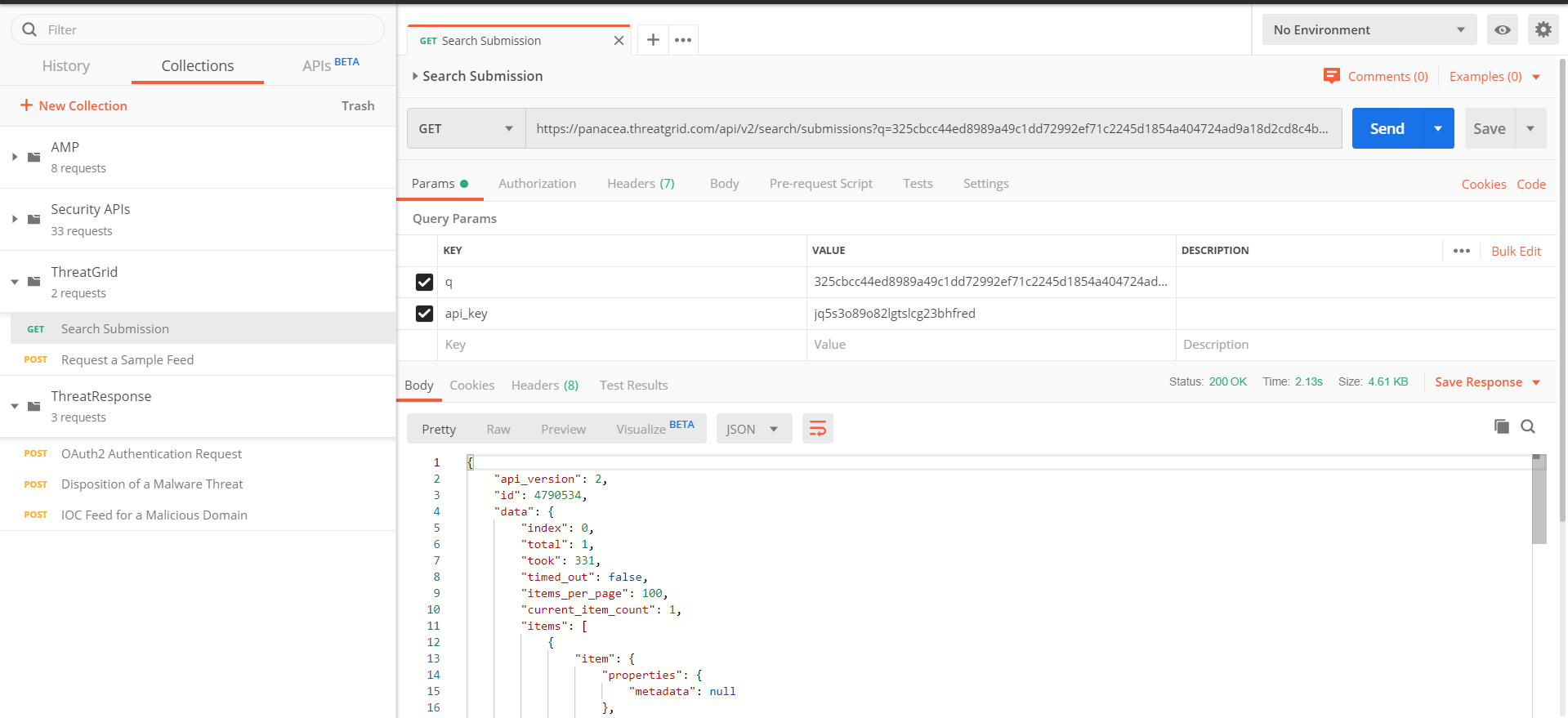


API\_KEY



API\_URL

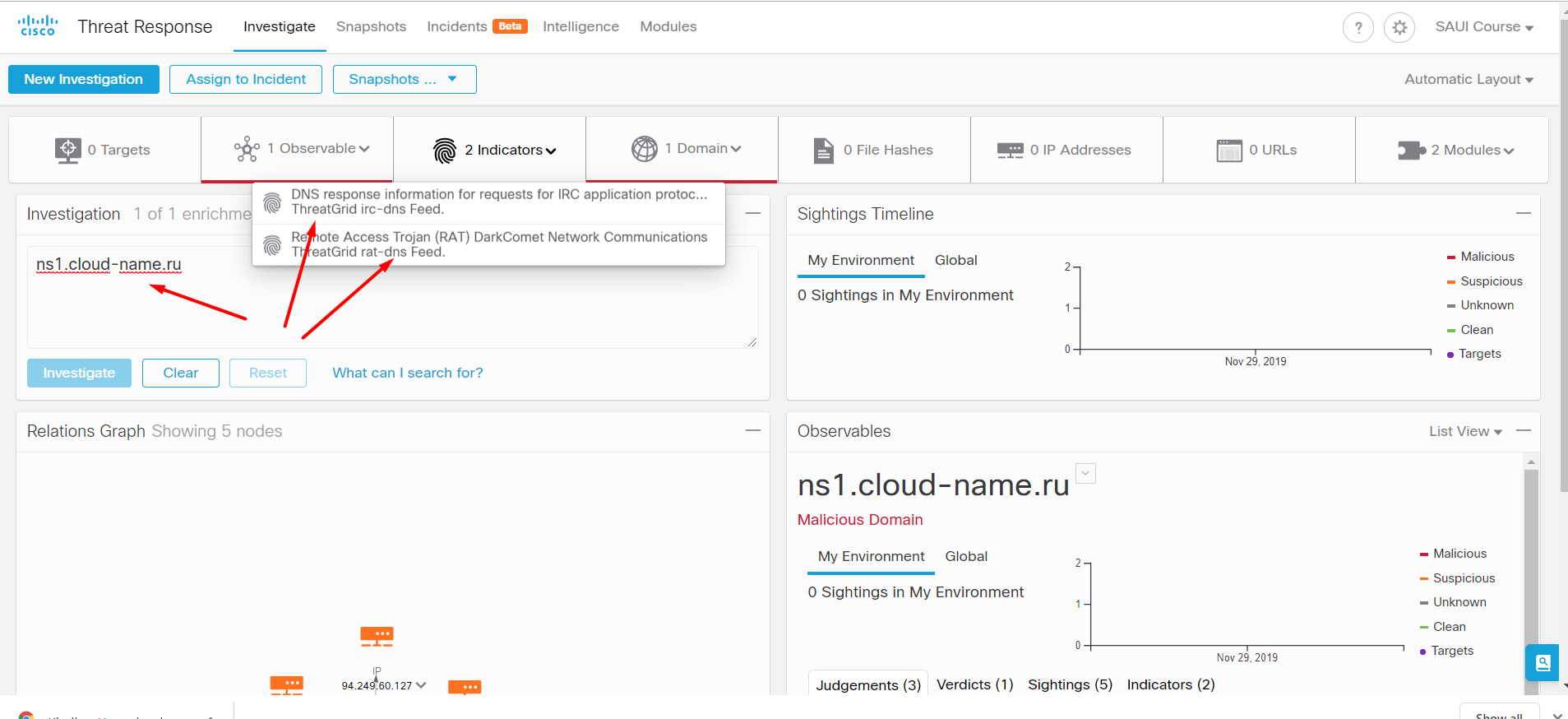




47) TG - Query the Indication of Compromise Feed for a Malicious Domain

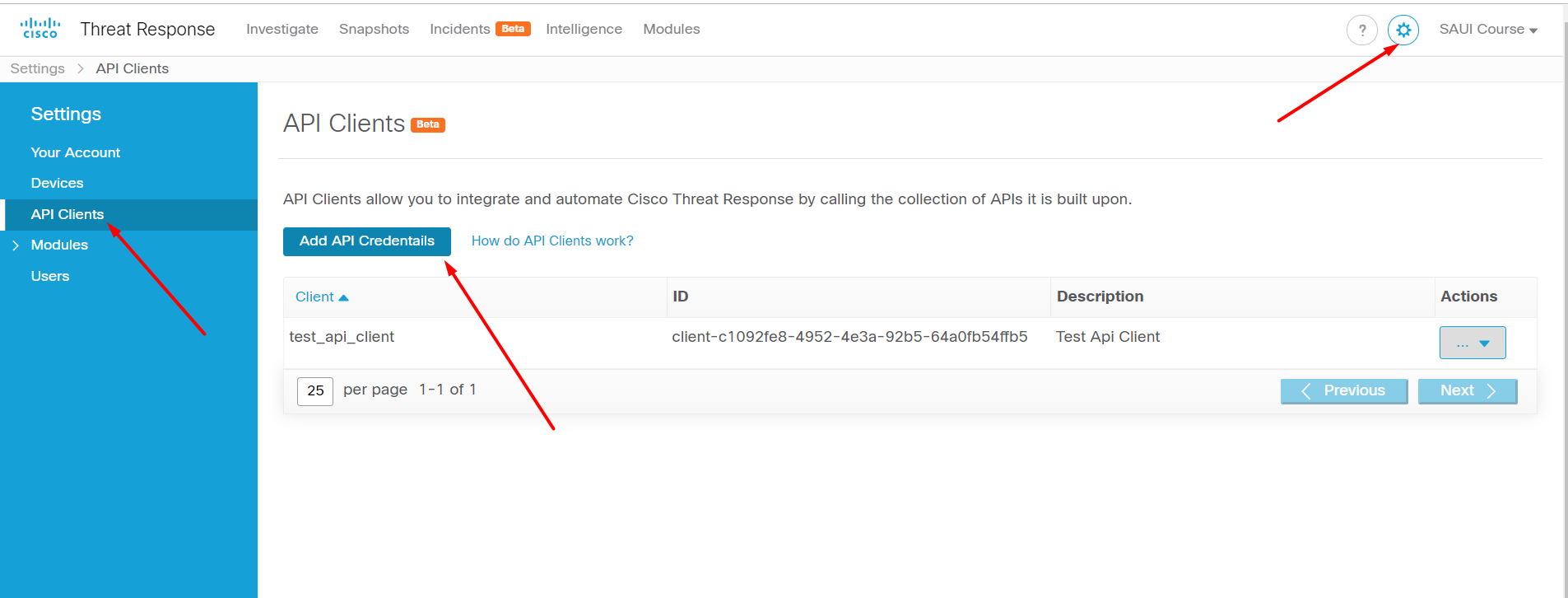
- On the site

<https://visibility.amp.cisco.com/investigate>

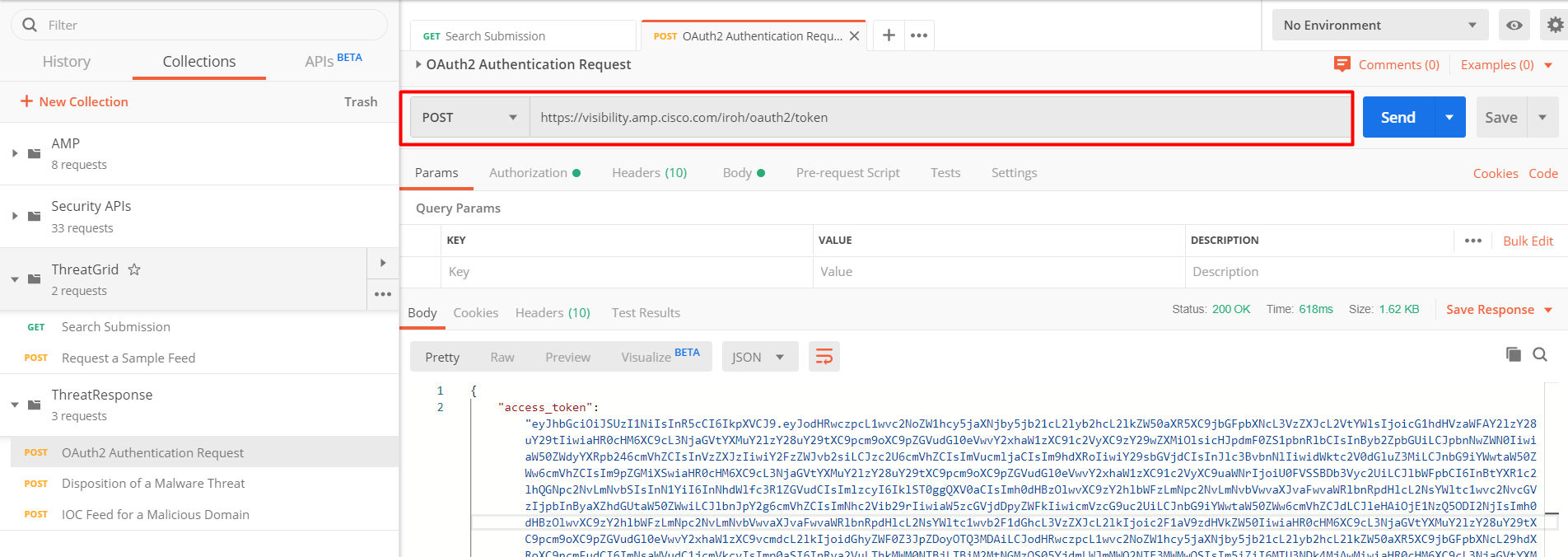


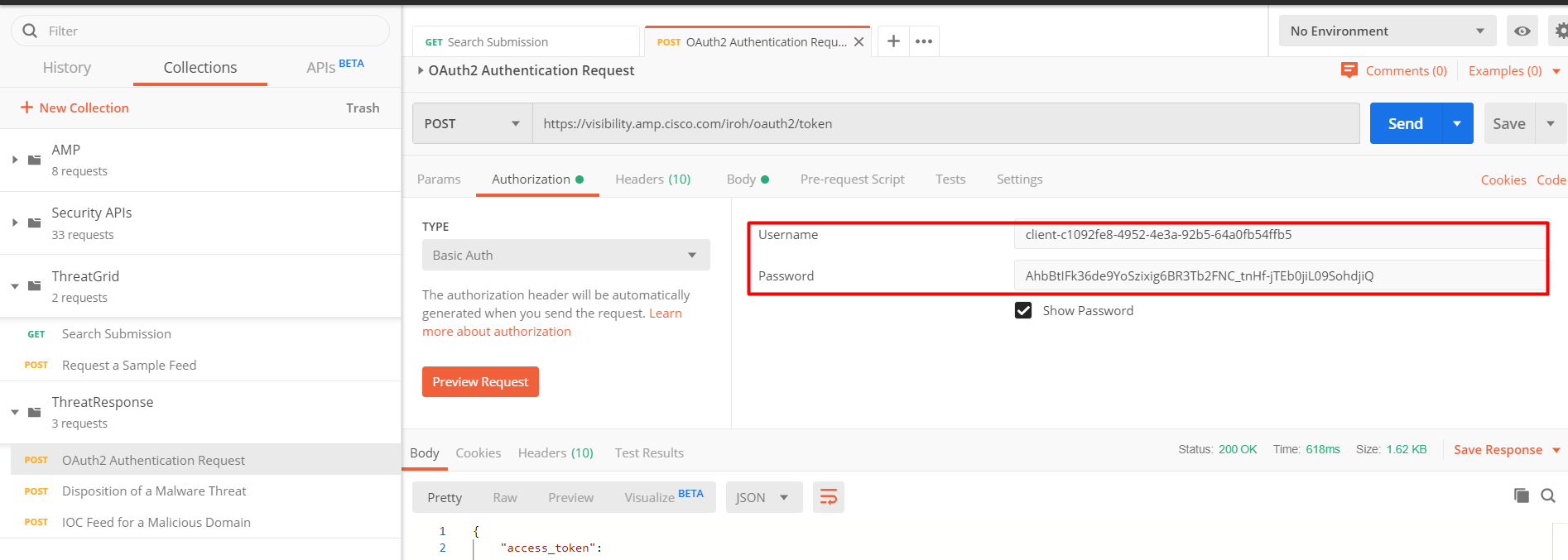
- Using the Postman

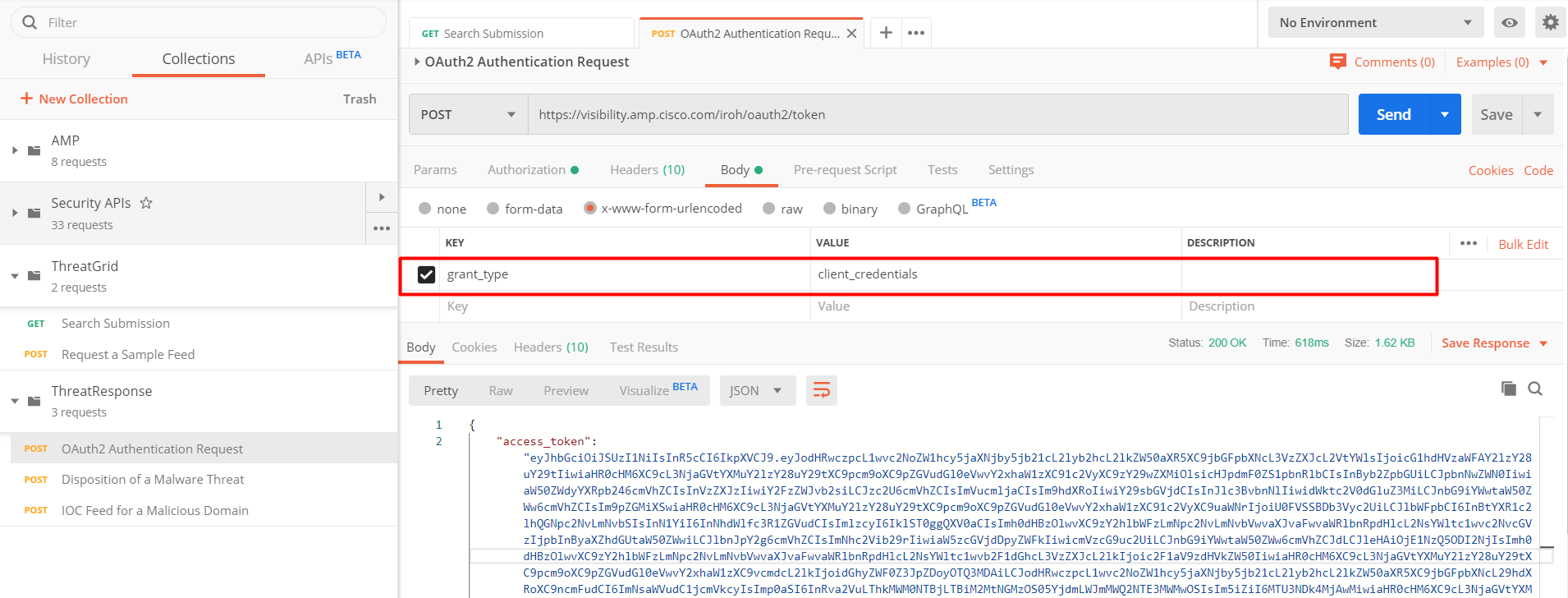
API key



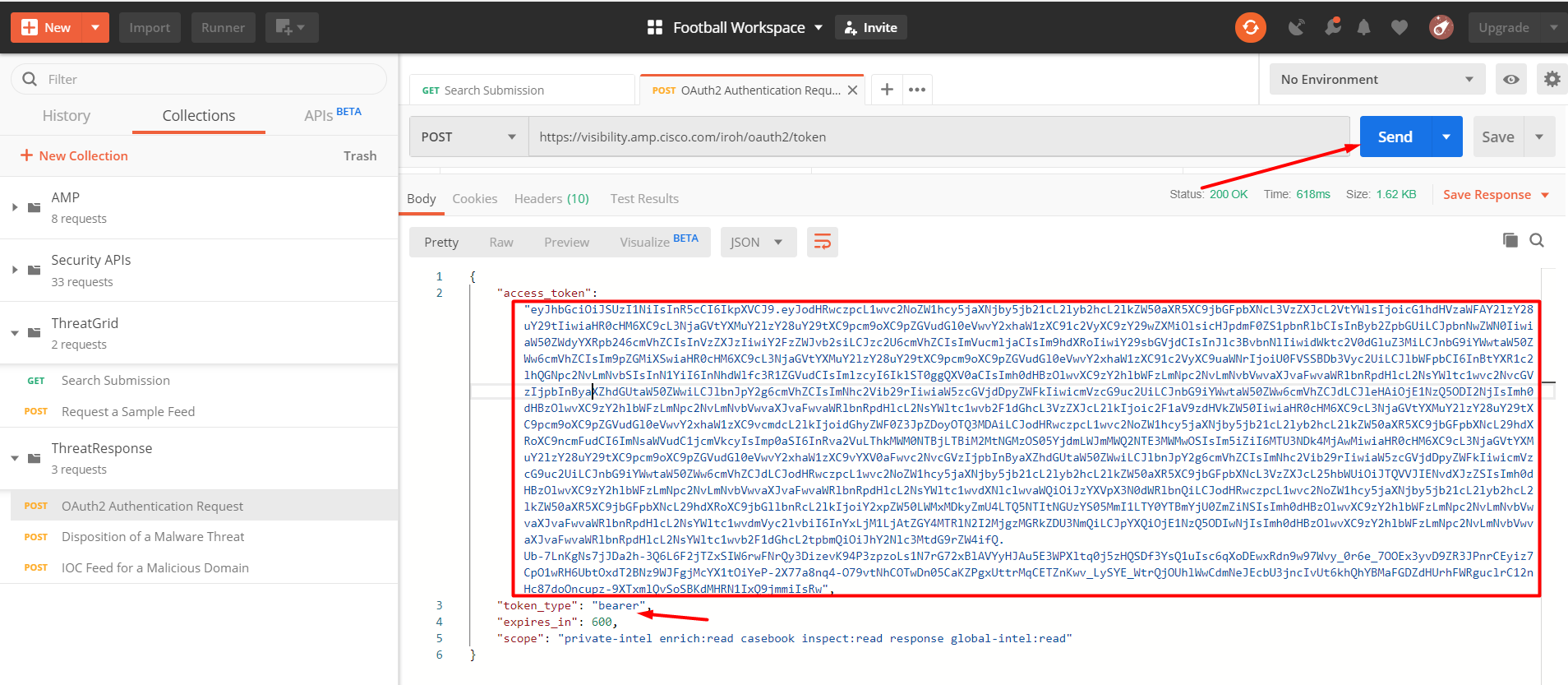
-Get the OAuth2 Authentication code



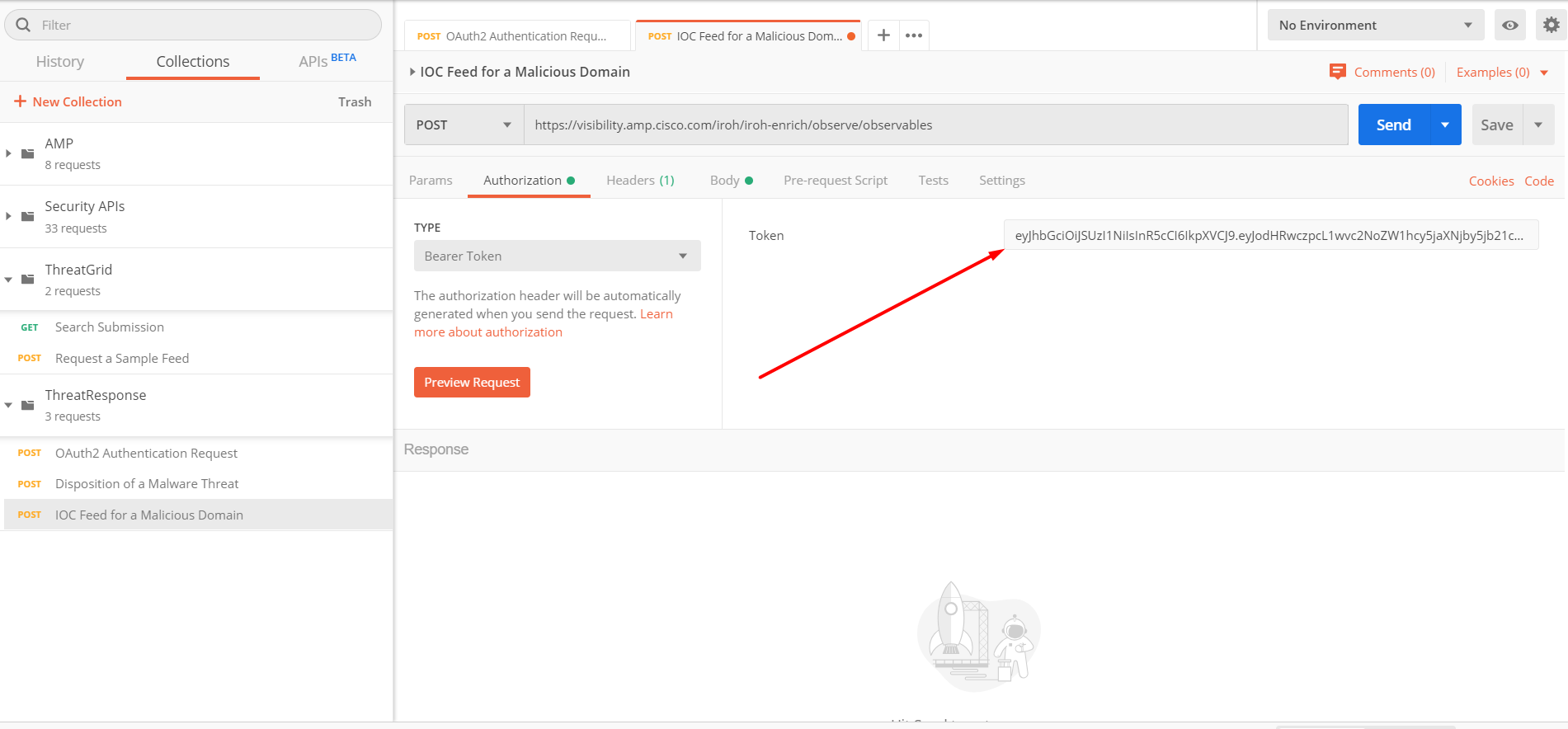


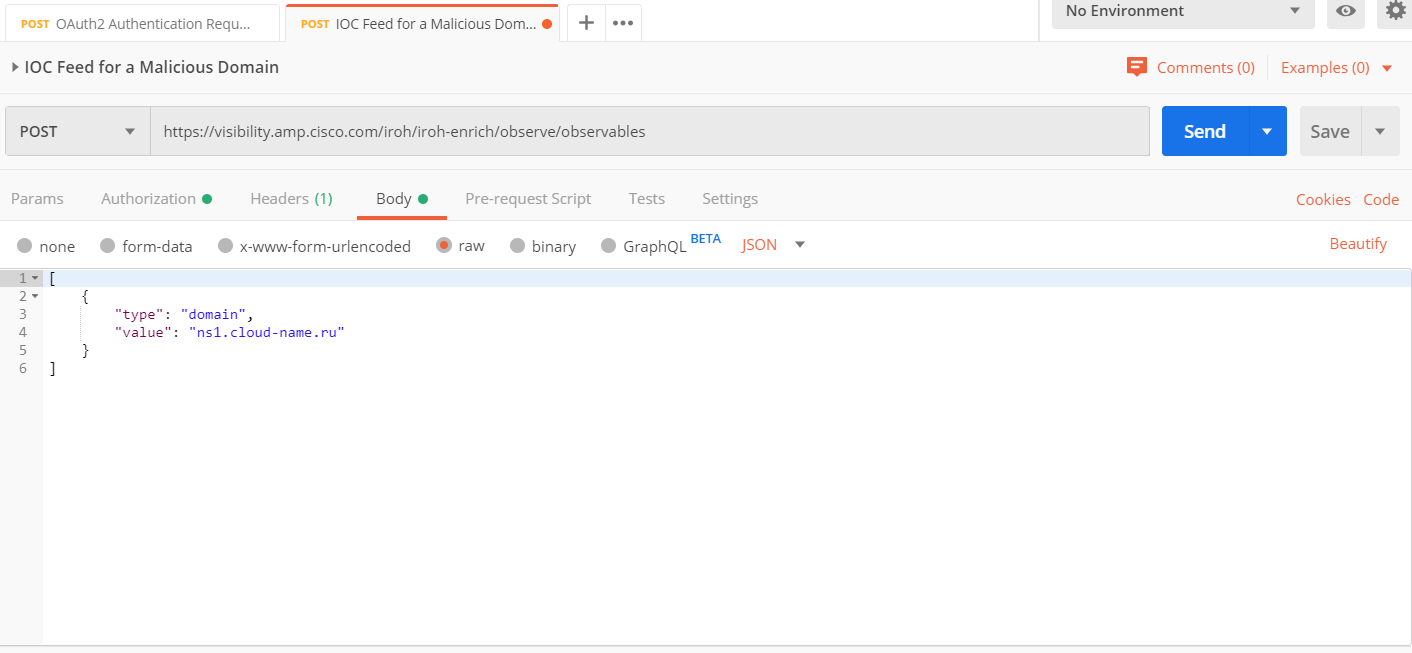


After clicking the “Send” button, copy the access token. This is bearer token.

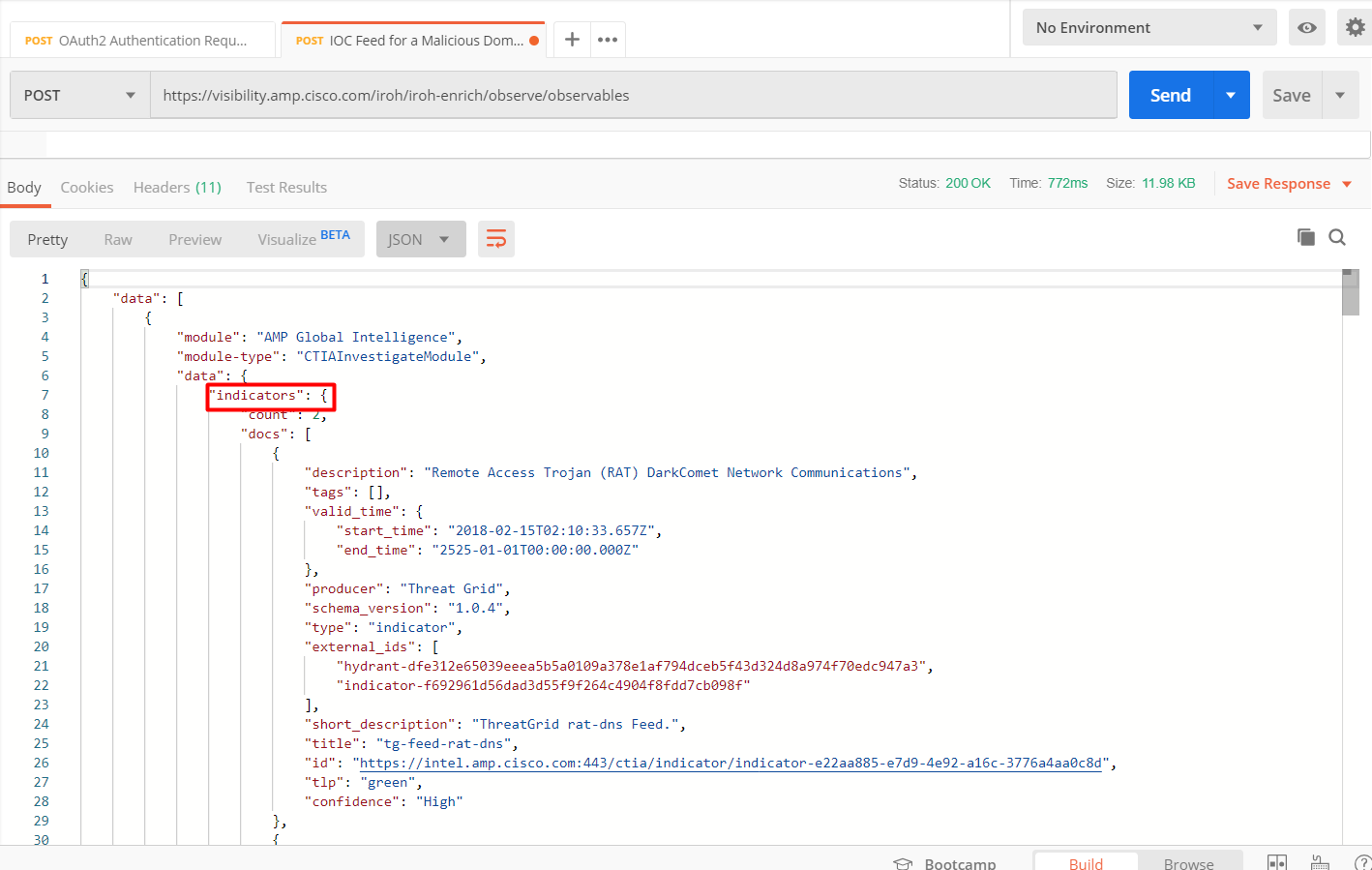


- Set the Authentication code when calling the “IOC Feed for a Malicious Domain”.

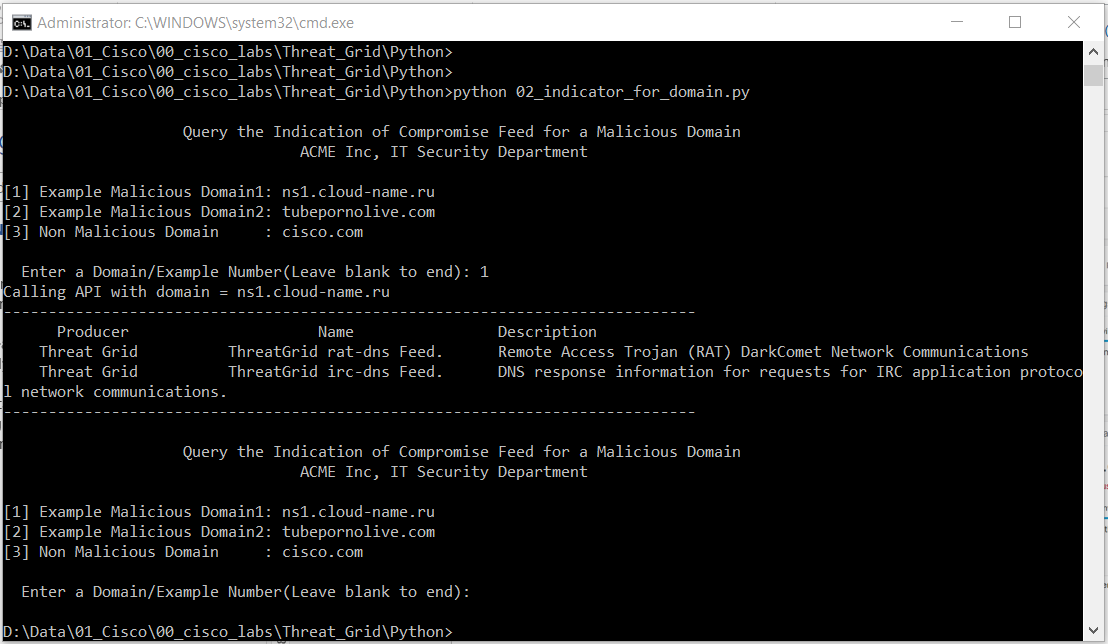




Result:



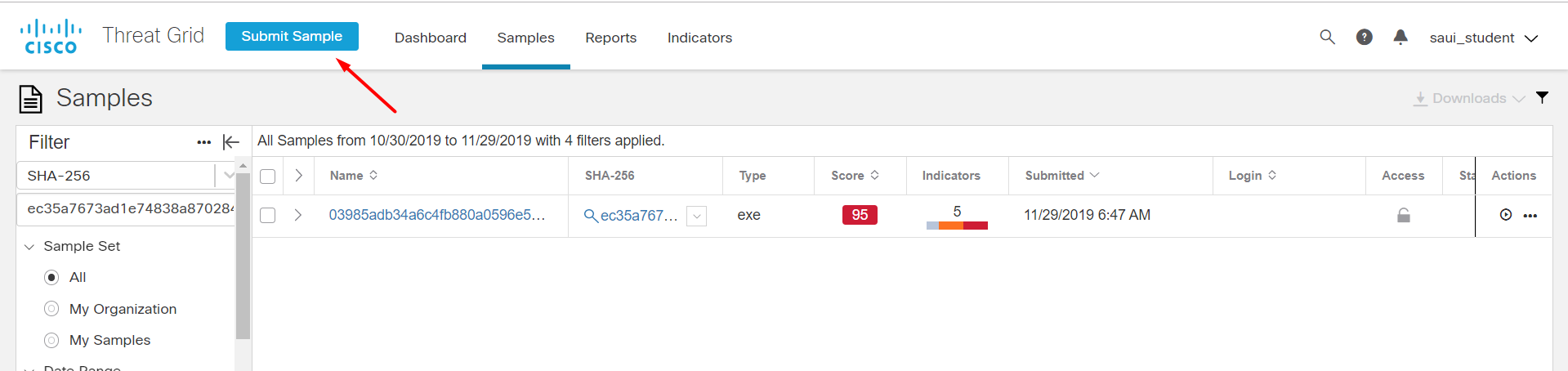
- Using the Python



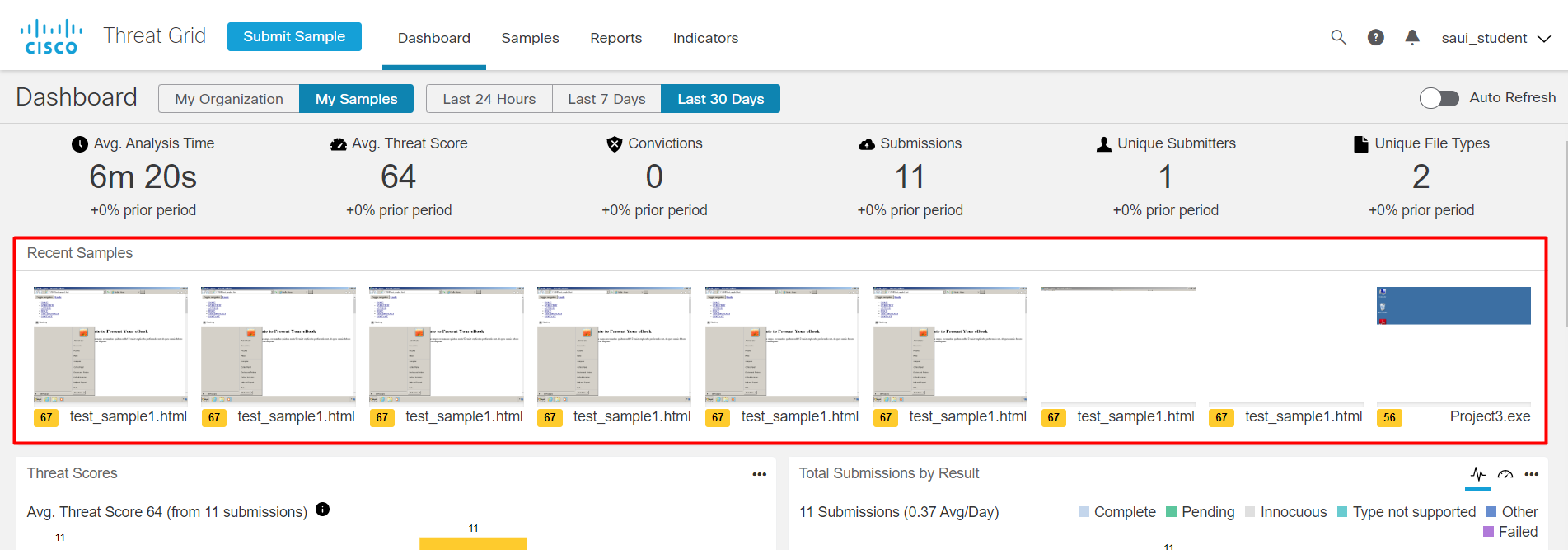
48) TG - Request with the API for Sample Feeds

- On the site

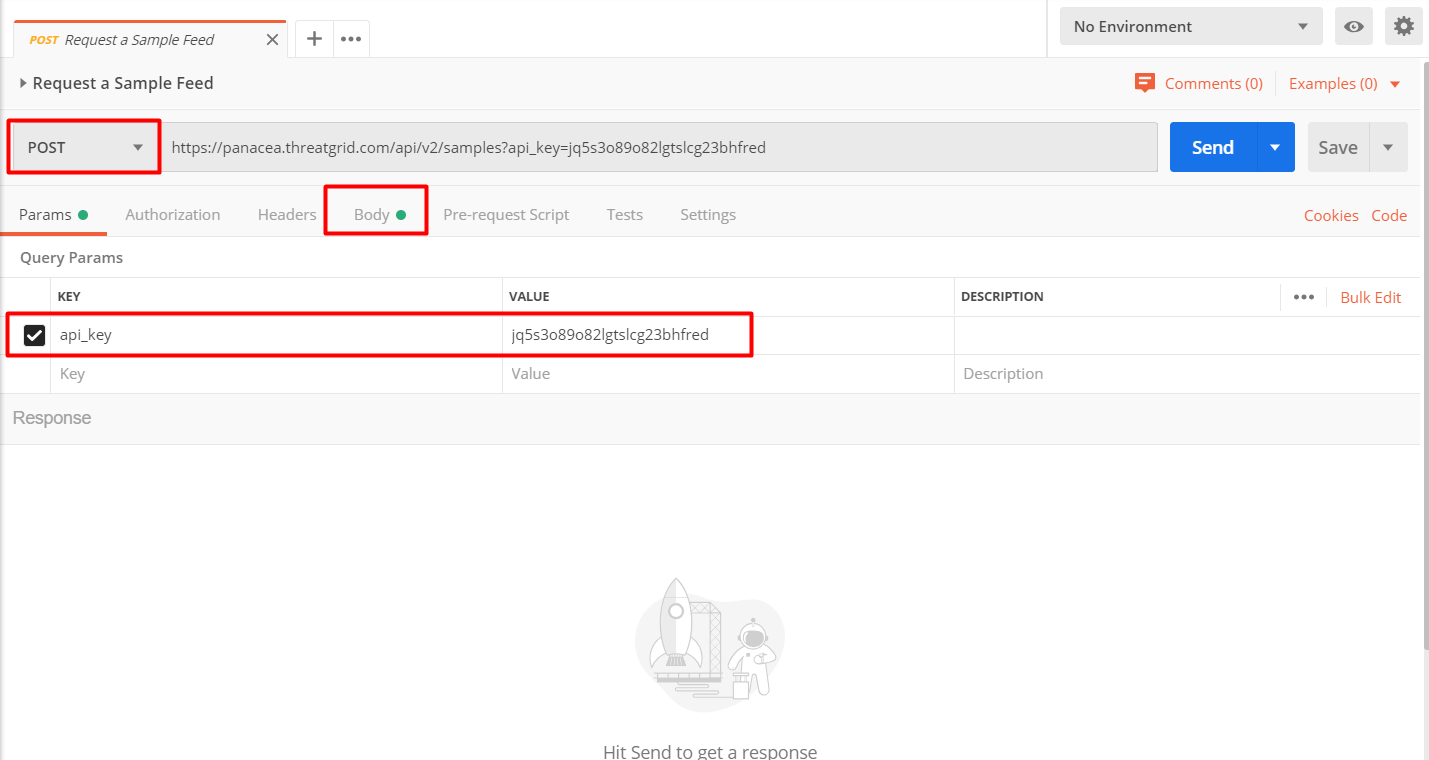
<https://panacea.threatgrid.com/mask/samples>

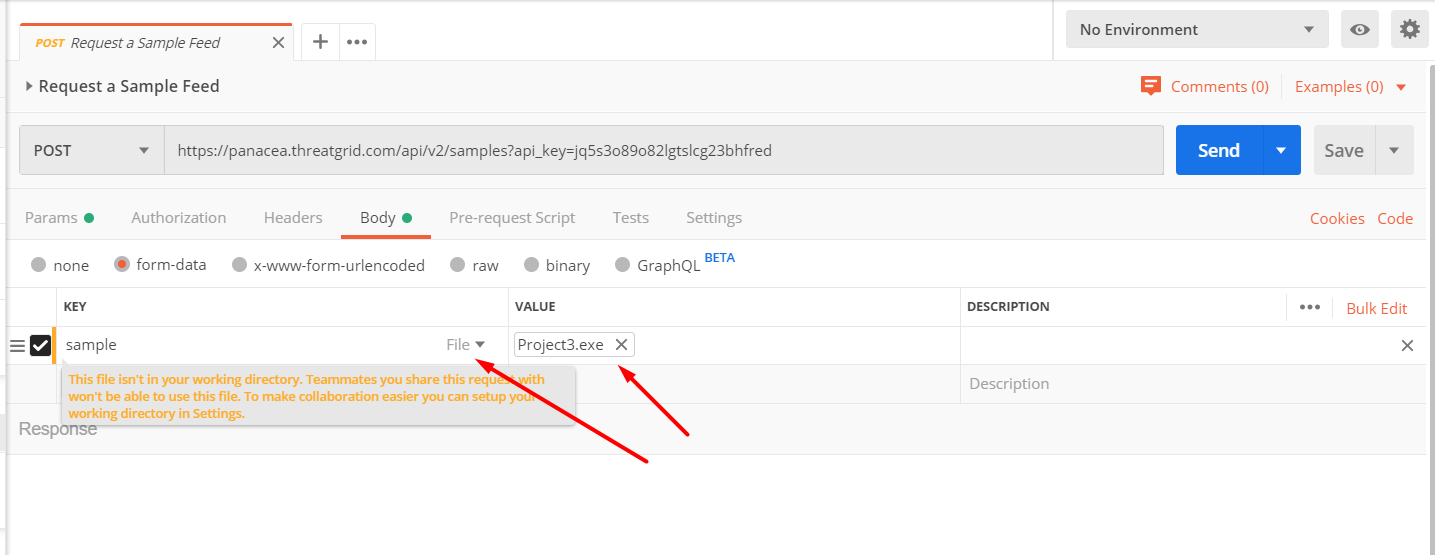


Reset result

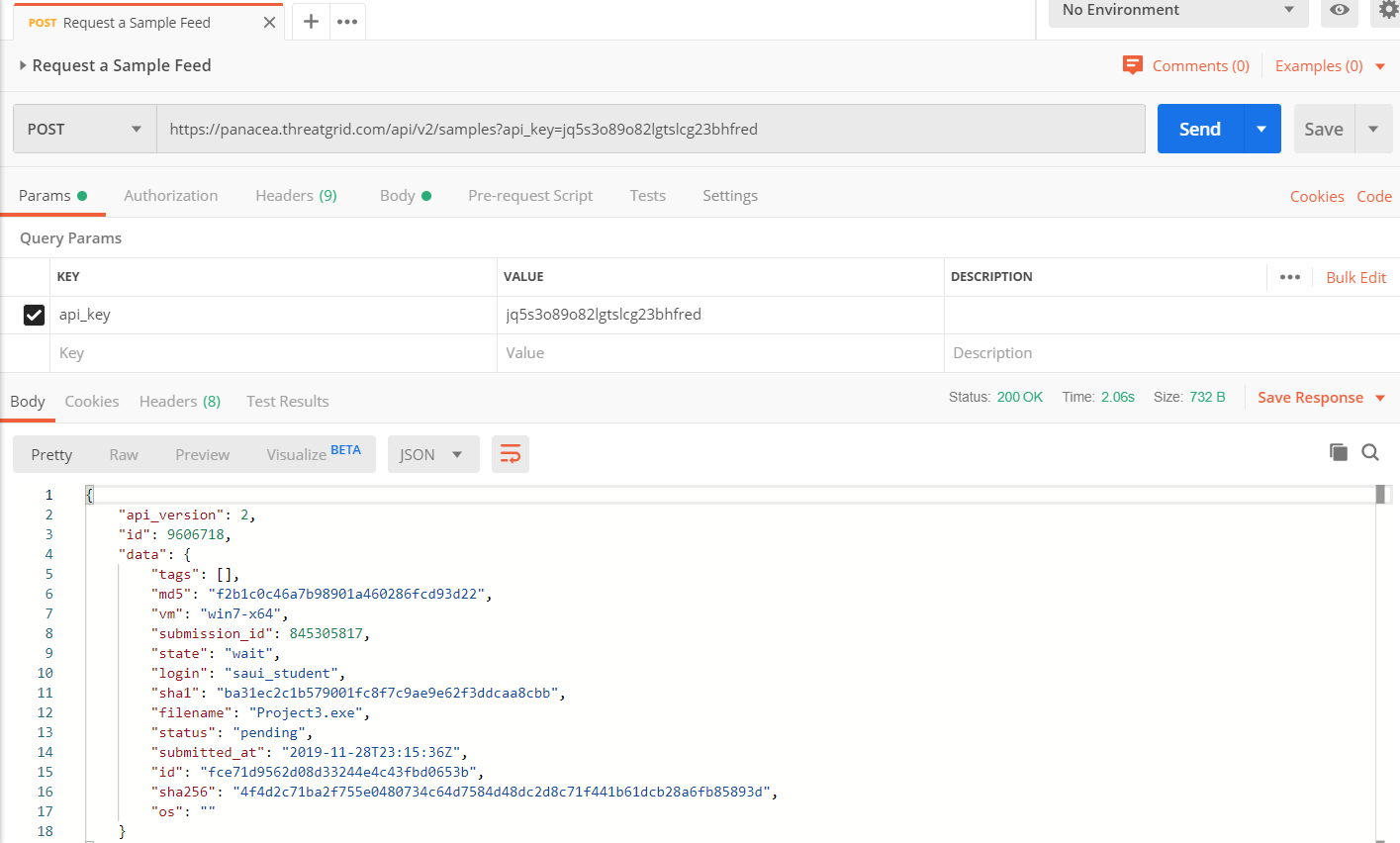


- Using Postman

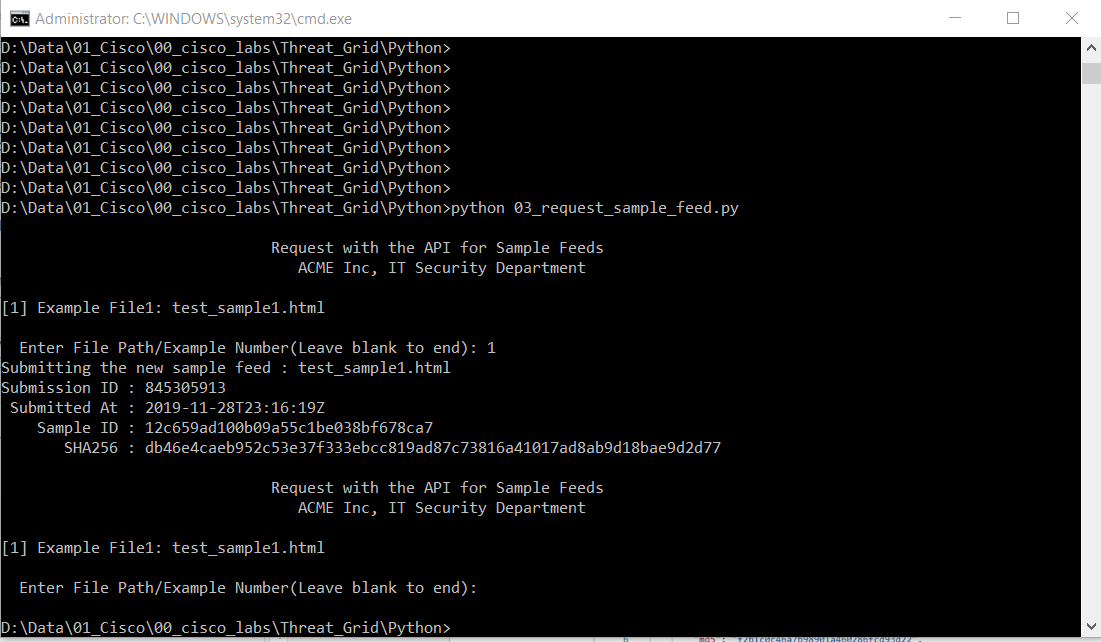




Result



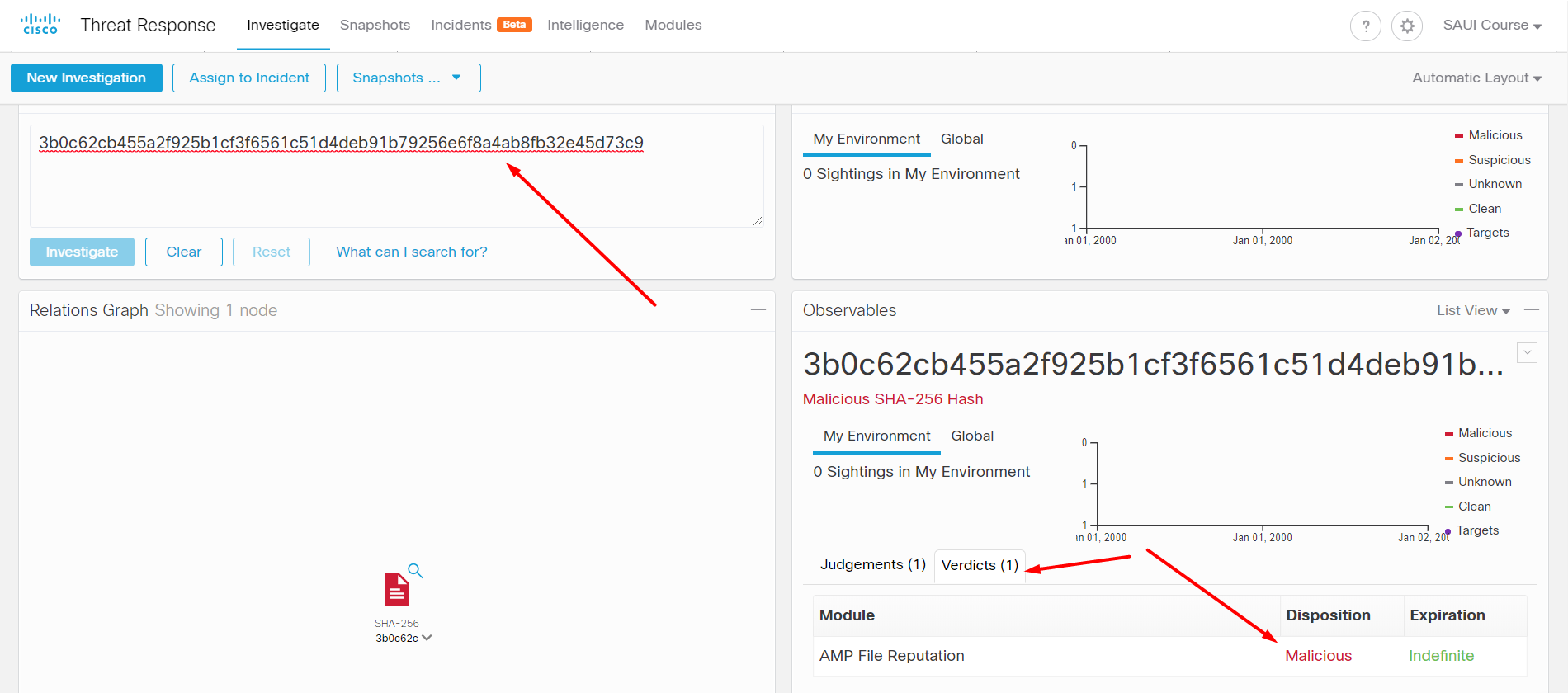
- Using the Python



49) TG - Disposition of a Malware Threat

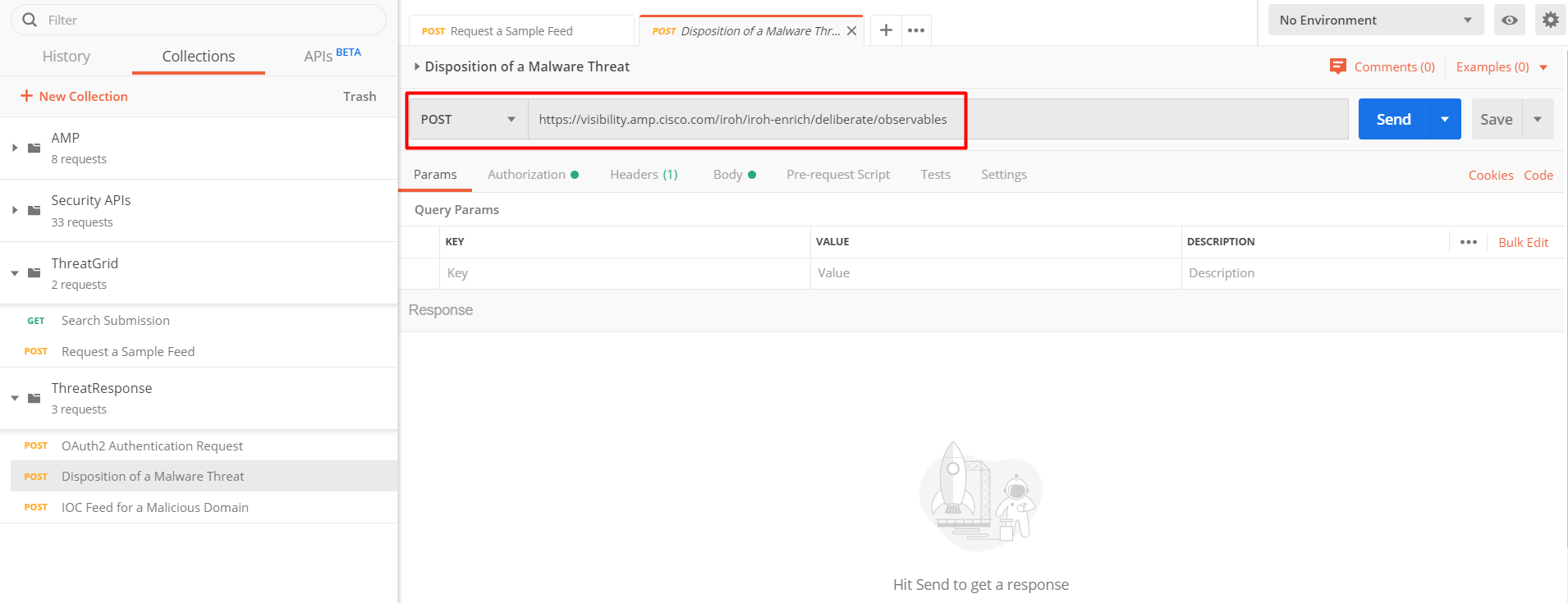
- On the site

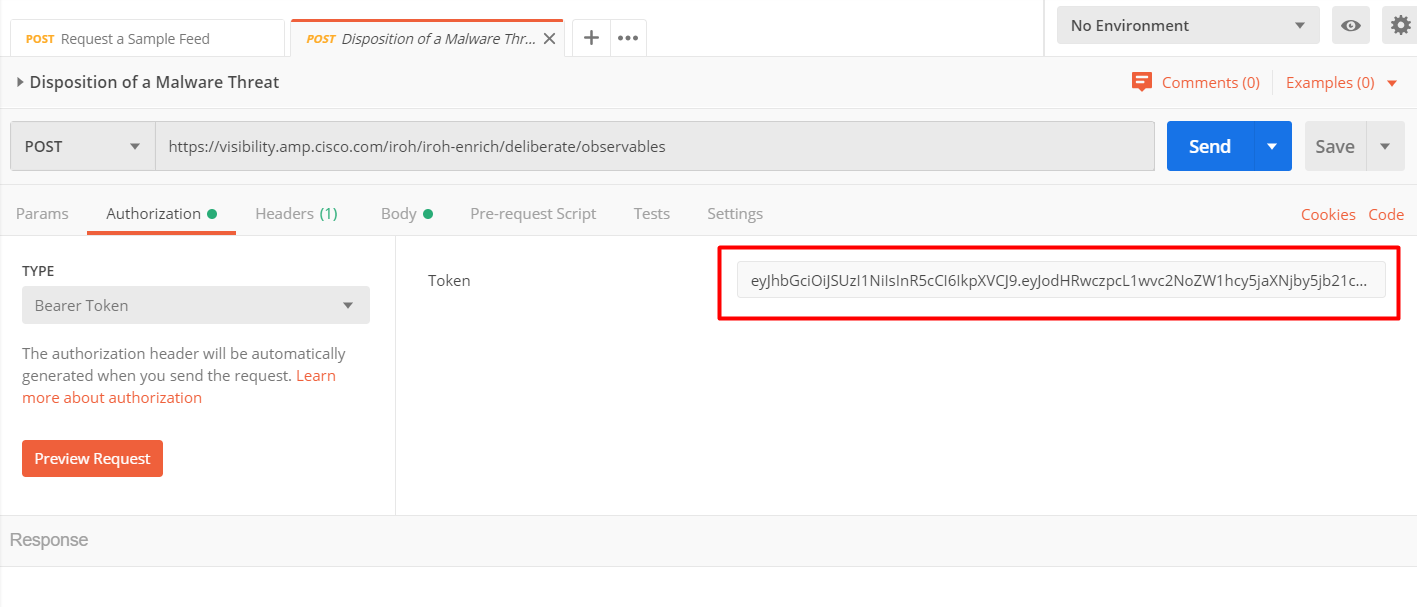
<https://visibility.amp.cisco.com/investigate>

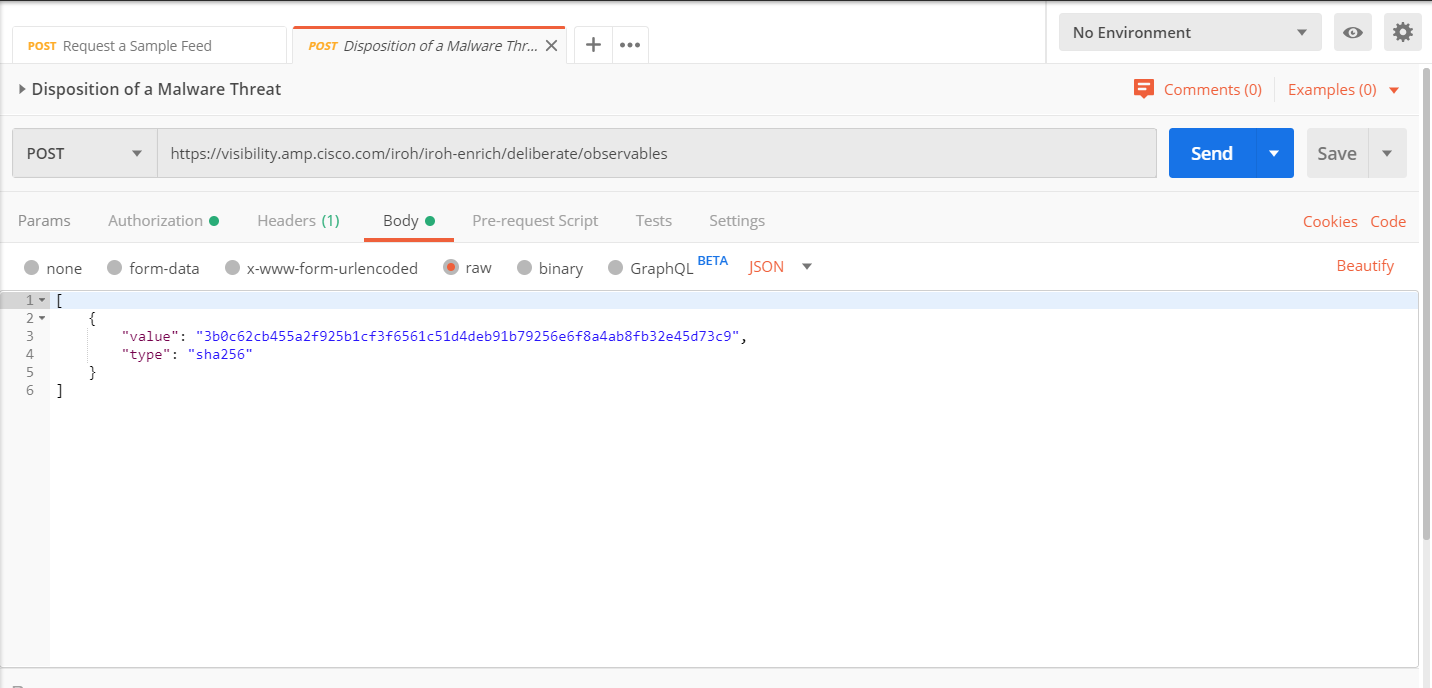


- Using the Postman

Get the OAuth2 authentication code and set it on the bearer code.







- Using the Python