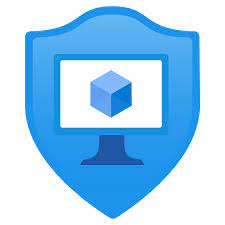
Are you tired of getting data from MS 365 Defender and put it in our tracker? Do you want to have an easy way to get it done like a pro? You are in the right place. So here, I offer you the internal tool nriapp. No information leaked on the software itself.

How does it work?

User need to log in to their account under tenant kwijp.onmicrosoft.com, the tool will retrieve (hijack) the session headers and cookies after the authentication.

The tool will use the cookies and the session to query the needed information with POST and GET HTTP methods. It works the same way with having API key but it only last approx. 8 hours so it requires to log again. T

Where can I get the software?

1. This tool is programmed using Python so you need to request first the Python3.7+ in AtYourService. You can use the miniconda which has Python3.9 by default.
2. Once you got the miniconda, you can install it directly by a single command line.

***pip install nriapp***

1. After the installation, you can setup your own tool. You may type the following in order to store the email address and output folder where the documents will be save.

***Python -m ChromeDriver –email=”Your email address” --output=”output folder”***

1. You can now query the incident id you wanted to investigate and it will automatically query all the need and important details in investigation.

This will automatically log you to MS 365 Defender and Endpoint Management. What you only need to do is put the OTP from email on the logon page and ready to go.

When the session expires, you only have to login again.

Requirements:

Python 3.8+ (Miniconda in AYS 3.9) – Request in AYS

