LAB1

Scenario

PurpleHawkS CISO came across few Threat Intelligence feeds and he want that Cybersecurity Analyst review two feeds that came from CISA and map it to Mitre ATT&CK format.

Threat Intelligence Feed

[1] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a

[2] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-201a

Exercise

As a cybersecurity analyst review the threat-intel links and map the TTPs using Mitre ATT&CK Navigator.

https://mitre-attack.github.io/attack-navigator/

Requirements:

1. Add color to TTPs.
2. Platform would be only “Linux or Windows” – Depending on TTPs.
3. Use “comment” for adding details on the technique.
4. Use selection controls to match the exact TTPs mentioned on the Intel.
5. Hide all unrelated TTPs.
6. Download in JSON or SVG format.