LAB3

Scenario

PurpleHawkS client sent us a Threat Group report, and Manager wants SOC Analyst to write a summary on gap analysis with identified TTPs for internal enrichment. Also, add the threat details on the database.

Threat Group using NetSupport RAT

https://thedfirreport.com/2023/10/30/netsupport-intrusion-results-in-domain-compromise/

Detection-Visibility file is added to GitHub

Exercise

As a cybersecurity analyst, review and collect all TTPs information on the threat group and conduct a gap analysis to improve detection and visibility.

Requirements:

1. Add the Group, Reference, Notes and TTPs to the database - Workbench.
2. Add Group to DeTT&CT
3. Run detect.py to compare the detection coverage and visibility.
4. Write a summary on your gap analysis.

Reference: https://medium.com/@chandrak.trivedi/purple-teaming-best-gap-analysis-open-source-tool-vectr-and-dettect-c969b19590c9