LAB7

Scenario

PurpleHawkS CISO wants to conduct a purple teaming exercise, and he wants a Security Engineer to plan the exercise and co-ordinate with the red/blue team.

Ransomware Attack

https://thedfirreport.com/2024/01/29/buzzing-on-christmas-eve-trigona-ransomware-in-3-hours/

Exercise

As a Security Engineer, review the TTP from the TI link and use an open-source purple teaming tool - VECTR to start planning the exercise and conduct gap analysis.

Requirements:

1. Create Campaign under PurpleHawkS and add TTP details.
2. Start adding Red Team details - Add any Five TTP as emulation adversary.
3. Start adding Blue Team Output - 2 Detected, 1 no alert, 1 logged and 1 no logs.
4. Review the report for Gap Analysis

Please Note: We will not perform emulation on a testing device but manually add blue side result just to get use to the tool.