LAB9

Scenario

Conduct a purple teaming exercise by referencing the Atomic Red Team for Emulation and creating Sigma rules with SigmaHQ guidance.

Atomic Red - TTPs: Atomics - Explore Atomic Red Team
Sigma Rule: sigma/rules/windows at master · SigmaHQ/sigma (github.com)

Exercise

As a Security Engineer, select TTP using Atomic Red and follow the purple teaming runbook by using Workbench, Caldera, VECTR and Threathound.

Requirements:

1. Add the TTP on Workbench.
2. Red Team - Emulation TTP using Caldera.
3. Purple Team - Exercise details on VECTR.
4. Export the logs from the Windows device.
5. Detection Engineering - Add detections.
6. Blue Team - Run the logs with ThreatHound against signatures created.
7. Gap Analysis Report.