LAB2

Scenario

PurpleHawkS CISO came across common adversary capabilities and he want that Cybersecurity Analyst write a summary on technical side and identify TTPs. Once completed, map to ATT&CK and D3FEND so that security posture is improved.

Adversary Capability

[1] https://thedfirreport.com/wp-content/uploads/2023/12/19208-007.png

[2] https://thedfirreport.com/wp-content/uploads/2023/09/18364-033.png

[3] https://thedfirreport.com/wp-content/uploads/2023/09/18364-036.png

[4] https://thedfirreport.com/wp-content/uploads/2023/09/18364-044.png

[5] https://thedfirreport.com/wp-content/uploads/2023/09/18364-056.png

[6] https://thedfirreport.com/wp-content/uploads/2023/08/18543-040.png

[7] https://thedfirreport.com/wp-content/uploads/2023/08/18543-025-1.png

[8] https://thedfirreport.com/wp-content/uploads/2023/05/18190-020.png

[9] https://thedfirreport.com/wp-content/uploads/2023/05/18190-022.png

[10] https://thedfirreport.com/wp-content/uploads/2023/02/17333-024.png

Reference: https://thedfirreport.com/

Exercise

As a cybersecurity analyst, identify the adversary capability and map the TTPs using Mitre ATT&CK Navigator and analysis D3FEND as countermeasures.

https://mitre-attack.github.io/attack-navigator/
https://d3fend.mitre.org/

Requirements:

1. Create layers and map the TTP from screenshots.
2. Co-related to countermeasures to improve security posture.
3. Write a summary of your analysis.