The MITRE ATT&CK Framework was inspired by the research paper “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains” by Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin. This paper introduced the “Cyber Kill Chain”, which if you’ve been following the SOC Level 1 path on TryHackMe you’ve already learned about. The MITRE ATT&CK Framework proves to maintain a place in any cyberspace and is a great source of information. Let’s get started!

Task 1

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework

CAR (Cyber Analytics Repository) Knowledge Base

ENGAGE (sorry, no fancy acronym)

D3FEND (Detection, Denial, and Disruption Framework Empowering Network Defense)

AEP (ATT&CK Emulation Plans)

Task 2

APT — Advanced Persistent Threat — A team/group or nation-state actor that engages in long-term attacks against organizations and/or countries.

TTP — Tactics, Techniques, and Procedures

Tactic — Adversary’s goal or objective.

Technique — How the adversary achieves the goal or objective.

Procedure — How the technique is executed.

Task 3

Question 3.1: Besides Blue teamers, who else will use the ATT&CK Matrix? (Red Teamers, Purpe Teamers, SOC Managers?)

Ans: Red Teamers