WHAT IS MITRE?

MITRE ATT&CK Framework (MITRE) is an open-source repository of information on adversary groups and the techniques they use to access, navigate, and exit protected systems. MITRE's database is accessible via their website, STIX, and Microsoft Excel. Additionally, cybersecurity teams can work with MITRE's data using ATT&CK Navigator, ATT&CK Workbench, and ATT&CK Python Utilities. Cybersecurity teams can use MITRE to research adversary groups, develop defenses against future attacks, and to analyze events post-attack.

Data and Tools:

MITRE's data is accessible through their website. There are two options to download the data:

- STIX- MITRE is available in STIX 2.0 and 2.1 and is for users who are proficient in Python
- Microsoft Excel- use MITRE in Excel for a more familiar user interface experience

There are three tools to customize the data for a specific team:

- ATT&CK Navigator- a GitHub-based tool that allows teams to navigate, annotate, and visualize MITRE's tactics
- ATT&CK Workbench- a GitHub-based tool that allows teams to build and manage a customized repository
- ATT&CK Python Utilities- a set of tools that allow teams to work with the data in Python

Organization:

MITRE has two key components: a library of adversary groups, their targets, and their preferred techniques; and a framework of tactics representing an adversary's goal, such as Initial Access, Persistence, and Defense Evasion. Each tactic contains numerous techniques that might be used to execute each potential stage.

There are three matrices containing different sets of tactics:

- Enterprise- used for platforms such as Windows, Linux, macOS, and SaaS
- Mobile- used for mobile devices such as Android and iOS
- ICS- used for ICS networks

Four Ways to Use MITRE:

MITRE can be used by cybersecurity teams of any experience level. Here are four ways teams can use MITRE to improve security:

- Detection and Analytics- create analytics to detect specific techniques that might be used by an adversary group

- Threat Intelligence- streamline communication by using a common language and being part of the threat intelligence community
- Adversary Emulation and Red Teaming- be the adversary and test defenses, find vulnerabilities and reduce the attack surface
- Assessment and Engineering- learn and assess how to use MITRE to protect the system

Resources:

MITRE ATT&CK. 2021. Accessed Oct. 20th, 2021. attack.mitre.org