MITRE ATT&CK Framework

Reading

1h

Status | Incomplete

Introduction

In this reading, you will learn what the MITRE ATT&CK framework is and how it is used by an SOC team to handle cyberattacks more effectively.

ATT&CK is a model developed by MITRE to record, document, and track various techniques attackers use throughout the different stages of a cyber attack to infiltrate your network and exfiltrate data. As explained by Trellix, **MITRE ATT&CK** stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). The MITRE ATT&CK framework is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target.

> Watch the video given here to get a quick overview of the MITRE ATT&CK framework.

The MITRE ATTACK architecture helps the Cyber Security team answer critical questions, such as how the attacker was able to break into the system and what they did once they were there. With the use of the reports that are produced by the MITRE ATT&CK, a company may figure out where in their security architecture there are flaws, as well as prioritize which flaws need to be fixed first based on the level of danger that each one poses.

> In the MITRE ATT&CK framework, **tactics** can be defined as the adversary's tactical goal: the reason for performing an action. For example, if the tactic identified is *Initial Access*, the adversary is trying to get into your network; if the tactic is *Discovery*, the adversary is trying to figure out your environment, etc.

MITRE ATT&CK has three iterations: ATT&CK for Enterprise, ATT&CK for Mobile, and ATT&CK for ICS. This page gives you all the tactics in the Enterprise iteration of ATT&CK.

Curious to learn more about MITRE ATT&CK? Jump to the next section to get an in-depth understanding of the MITRE ATT&CK framework.

Readings

1. The resources given below help you understand the MITRE ATT&CK framework from the foundational level; to begin, start with *ATT&CK 101 blog post*. Also, don't forget to add these to your (PKM) for future references:

- Getting Started | MITRE ATT&CK
- Getting started with ATT&CK

2. Use the following resource to understand different perspectives of the MITRE ATT&CK. You are advised to follow along with the instructions given in the reading: What Is MITRE ATT&CK and How to Use It for Self-Advancement?

   While going through this resource, focus on:

   - General Guidance: to understand the usage of ATT&CK technique and its application in the real-world.
   - Attack Navigator: this is a very helpful tool used to visualize the type of defense gaps or coverage an organization may have.
3. Familiarize yourself with the official MITRE website that you will be using throughout your Cyber Security professional career. Focus on analyzing the ATT&CK matrix for Enterprise and extracting the information you need from the matrix. ATT&CK Matrix: https://attack.mitre.org/#

> In addition to the ATT&CK website, this Trellix web-page would also be helpful, particularly in understanding the ATT&CK matrix.

Conclusion

In this reading, you learned the basics of the MITRE ATT&CK framework and how it is used for the purpose of incident response. In the next reading, you will learn what ATT&CK mappings are and how to work with these mappings.

Further Reading

Here is a reading to help you understand how the Cyber Kill Chain Model, Diamond Model, and ATT&CK framework compare with each other: CyCraft Classroom: MITRE ATT&CK vs. Cyber Kill Chain vs. Diamond Model.

✓ Mark Completed

Previous
Diamond Model for Intrusion Analysis

Next
Mapping to MITRE ATT&CK

W07D5

Fri Aug 9

- Outline & Notes (1)
- Lectures (1)
- Work (5)

5 hrs

- Using Strategic Intelligence on Carbanak Report
- Diamond Model for Intrusion Analysis
- MITRE ATT&CK Framework
- Mapping to MITRE ATT&CK
- Models & Frameworks Exercise

Other (1)

W07D5 Schedule »