MITRE ATT&CK® Framework

The war against Ukraine breaks out in five domains embracing land, sea, air, space, and cyberspace. The attacks escalating in the cyber domain impact not only Ukraine but bring the entire world to the brink of global cyber war. Nowadays, the main goal of Ukraine is to be the “shield of cyber defense” for the entire world, which will remain a crucial mission even after the Ukrainian victory in the ongoing war.

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private & public sectors as well as in the cybersecurity product and service community.

The MITRE ATT&CK framework is based on the Lockheed Martin Cyber Kill Chain®. The Cyber Kill Chain concept was invented by Lockheed Martin, an aerospace, arms, defense, information security, and technology corporation acting as the U.S. largest defense contractor. The methodology was created in accordance with the U.S. military doctrine that presumes five domains of war, including cyberspace.

The ATT&CK framework is very similar to the periodic table in chemistry. It helps to profile, identify, and compare threat actors’ tactics, techniques, and procedures (TTPs) acting as a universal methodology to analyze cyber attacks and prioritize threat detection goals.

Currently, MITRE ATT&CK is widely adopted across the cybersecurity industry to classify cyber attacks, identify attribution and objectives, assess organizations’ risks, and prioritize cyber defense activities. Also, the framework is used to tag detection algorithms written in Sigma language to provide a clear understanding of what exactly to detect in your organization.

MITRE ATT&CK®: Analyzing and Attributing Cyber Attacks

The course objective is to learn the theoretical basics of MITRE ATT&CK and apply the framework in practice to analyze cyber attacks, identify threats, and prioritize cyber defense activities.

- MITRE ATT&CK: History of evolution and core principles
- Types of matrices and their structure
- Tactics, techniques, and sub-techniques
- Areas of application & methodology, Sigma rules tagging with MITRE ATT&CK
- Practical use cases of attack analysis
- MITRE ATT&CK tools, including ATT&CK Navigator

What We Offer

- Guest lectures by seasoned SOC Prime experts
- Self-advancement materials available online
- Direct access to SOC Prime resources to hone practical skills

The best students might be offered grants for Sigma rules and MITRE ATT&CK Defender (MAD) certifications, an internship at SOC Prime, and other educational grants.