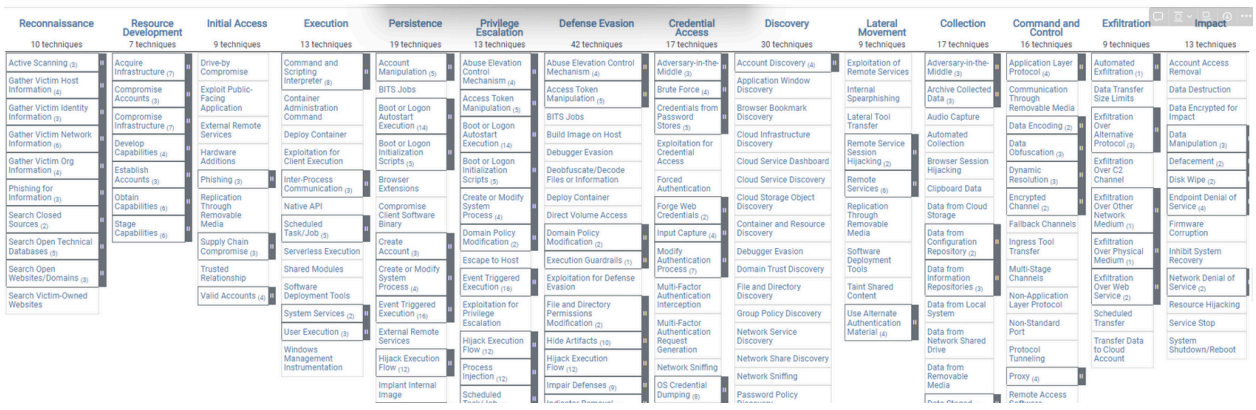
Introductory Information About MITRE Course

Cyber attackers have been performing cyber attacks on systems using the attack vectors of the time since digital systems existed. In the past, cyber attacks consisted of simple and understandable attack methods, as there were no complex and large digital systems. **But over time, digital systems have grown and evolved into more complex digital structures, so cyber attacks have also become more difficult to understand with advanced methods.** This also makes it difficult the detection of cyber attacks. Today, in order to fully understand a cyber attack, it is necessary to model the steps and details of cyber attacks in a way that is suitable for certain groups. One of the important frameworks that meets this modeling need is the MITRE ATT&CK framework.

Introduction to MITRE

What is MITRE?

MITRE was founded in 1958 in the USA. as an organization that produces innovative solutions to advance national security in new ways and serve the public interest as an independent adviser. MITRE's areas of work are Cybersecurity, Aerospace, AI & Machine Learning, Aviation & Transportation, Defense & Intelligence, Government Innovation, Health, Homeland Security and Telecom.



What is MITRE ATT&CK Framework?

MITRE ATT&CK that stands for Adversarial Tactics, Techniques, and Common Knowledge is the framework of a knowledge database that was introduced by MITRE in 2013 and has been continuously developed and expanded along with the technology.** It is possible to analyze cyber attacks systematically through the MITRE ATT&CK framework. Cyber attacks can be divided into certain stages and the methods used in each stage can be analyzed in depth and used in studies related to cyber security. The MITRE ATT&CK Framework is an essential resource for each and every employee in the cybersecurity industry.

Why is the MITRE ATT&CK Framework important to SOC Analysts?

Since each step of cyber attacks is covered in detail in the MITRE ATT&CK Framework, SOC Analysts can clearly see the actions that should be taken for each stage of the cyber attack and that it as a reference. In this way, attack detection and mitigation techniques developed against cyber attacks can be used more effectively, cyber attacks can be mapped, an in-depth report can be written and the details of the attack can be archived for a later use. Since this framework provides a clear roadmap of cyber attacks, researches can be conducted on other possible cyber attacks that have not yet occurred yet to develop ways to detect or avoid them.

What is MITRE ATT&CK Matrix?

MITRE ATT&CK Matrix is a visualization method used to classify and see attack methods of cyber attackers. Matrices can be customized for almost any subject and turned into useful visuals. MITRE has created MITRE ATT&CK matrices to visualize the details of attacker behavior using the matrices.

Types of Matrices

3 different matrices have been created within the MITRE ATT&CK Framework according to the platform types:

- Enterprise Matrix
- Mobile Matrix
- ICS (Industrial Control Systems) Matrix

Enterprise Matrix

Enterprise matrix is the first matrix created by MITRE. There are more digital systems included in this matrix and are more common than those that are included in other matrices, so there are a lot more information in this matrix than other matrices. Enterprise matrix is mainly used to understand the cyber attacks on large organizations

There are 7 sub-matrices under the Enterprise Matrix:

- PRE
- Windows
- macOS
- Linux
- Cloud
- Network
- Containers

Enterprise Matrix - https://attack.mitre.org/matrices/enterprise/

Mobile Matrix

The mobile matrix is the one that was prepared for mobile devices and contains information about the cyber security of mobile devices. This matrix can be used to ensure the security of individual and corporate mobile devices. Comparing the Enterprise Matrix, it contains less information:

Mobile Matrix

Mobile Matrix has 2 sub-matrices:

- Android
- iOS

ICS Matrix

The ICS Matrix is the one that contains the information collected for the cyber security of devices in the industrial control systems. This matrix can be used to provide cyber security and analyses of an ICS.

What is Tactic?

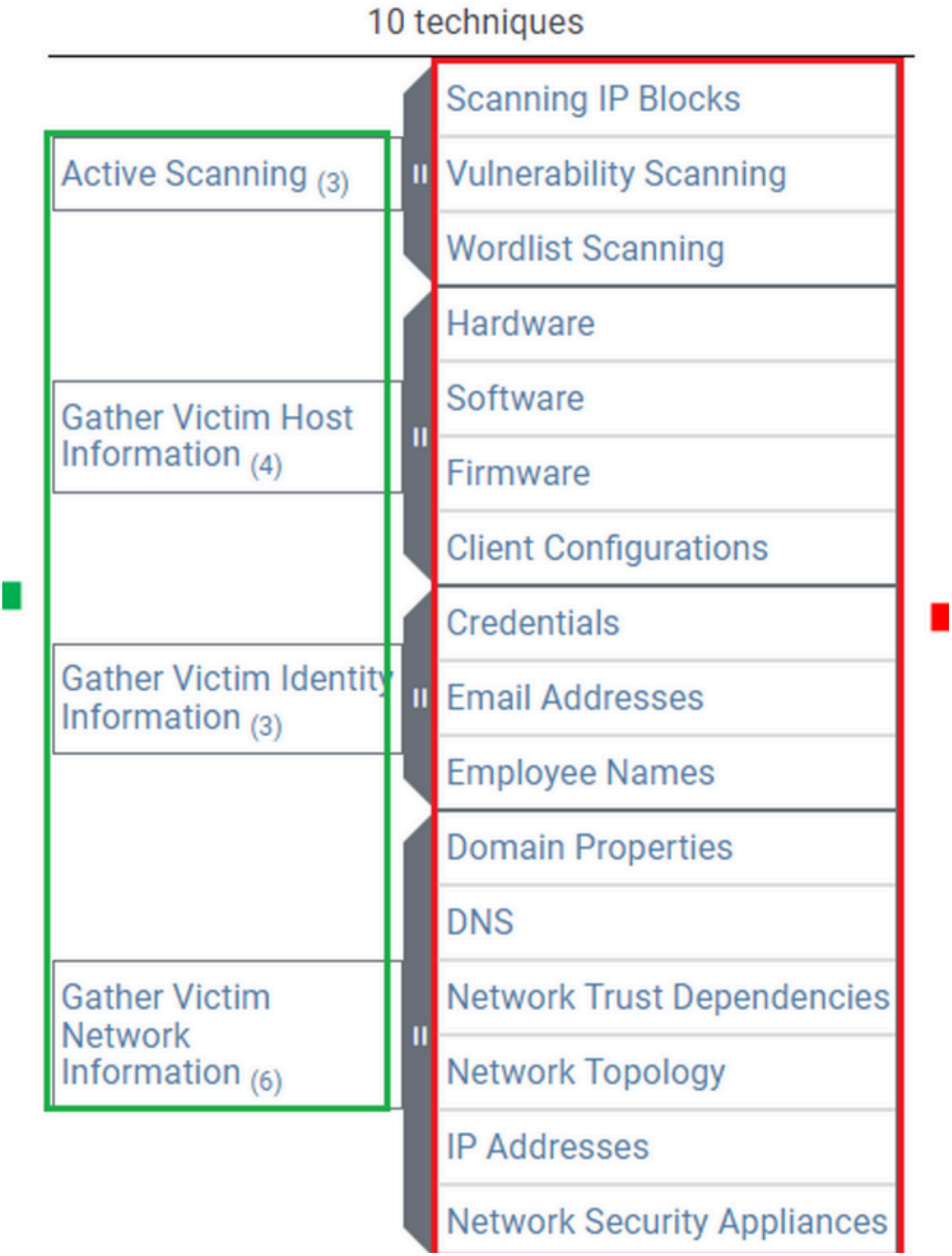
Tactic expresses the purpose of the cyber attacker and the reason for his action. Tactics are one of the most important MITRE ATT&CK Framework components used to group cyber attacker behaviors and see the attack steps. Tactics are in the top row of the matrix.

Types of Tactics

Tactics often consist of general statements as they express the purpose and reason for the cyber attack. Therefore, the tactics for each matrix are highly similar.

The tactic numbers and names in each matrix are given in the titles below.

The tactics within the matrix only show what the attackers aim and do not contain detailed information about the attacker's attack method. The techniques and sub-techniques, on the other hand show the methods used by the attacker to achieve his goal and how he conducted the attack exactly.


10 techniques
Active Scanning (3)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Scanning IP Blocks
Vulnerability Scanning
Wordlist Scanning
Hardware
Software
Firmware
Client Configurations
Credentials
Email Addresses
Employee Names
Domain Properties
DNS
Network Trust Dependencies
Network Topology
IP Addresses
Network Security Appliances

What are Techniques and Sub-Techniques?

Techniques and Sub-Techniques

As it is shown in the image above, If there are gray areas next to the boxes where the names of the techniques are written in the matrix, It indicates that the technique has a sub-technique. For example, let's see the sub-techniques of the first 4 techniques under the "Reconnaissance" tactic:

Types of Techniques and Sub-Techniques

Techniques are divided into 3 groups according to matrices:

- Enterprise Techniques
- Mobile Techniques
- ICS Techniques

Enterprise Techniques

There are quite a number of enterprise techniques and are constantly updated over the time. The current number (10.05.2023) of enterprise techniques and sub-techniques is as follows:

Techniques - 193

Sub-techniques- 01

You can check the current numbers at the link below:

Enterprise Techniques and Sub-techniques - https://attack.mitre.org/techniques/enterprise/

Mobile Techniques

Total number of mobile techniques is less than the enterprise techniques and they are updated over the time as well. The current number (10.05.2023) of the mobile techniques and sub-techniques is as follows:

Techniques - 66

Sub-techniques -41

You can check the current numbers at the link below:

Mobile Techniques and Sub-techniques - https://attack.mitre.org/techniques/mobile/

Mitigations

What are Mitigations?

Mitigations refers to **the measures and actions that can be taken in response to the techniques** in the MITRE ATT&CK matrix. Each mitigation has a unique ID, name and description that provides clear understanding about them. For example, the image below shows one of the enterprise mitigations:

Types of Mitigations

Mitigations are grouped into 3 for the matrices as in other MITRE ATT&CK components:

- Enterprise Mitigations
- Mobile Mitigations
- ICS Mitigations

Enterprise Mitigations

Mitigations - 43

You can check the below link to see the updated number:

Enterprise Mitigations - https://attack.mitre.org/mitigations/enterprise/

Mobile Mitigations
(Image Source: mitre.org)

Mitigations -11

You can check the below link to see the updated number:

Mobile Mitigations - https://attack.mitre.org/mitigations/mobile/

ICS Mitigations

The number of ICS mitigations at the time of preparation of this training is as follows:

Mitigations - 51

You can check the below link to see the updated number:

CS Mitigations https://attack.mitre.org/mitigations/ics/

Groups

Advanced Persistent Threat (APT) Groups, are the hacker groups that may include many different people and groups that carry out cyber attacks in a targeted and systematic way, with governments support from time to time. APT groups may conduct cyber attacks with different motivations. For example, the group may have a specific mission, may be conducting their attacks for money, or may be foreign government supported and conduct their attacks to obtain their national ideals.

Within the MITRE ATT&CK Framework, information about APT groups is collected which helps identify which APT group is targeting which systems and which cyber attack techniques are being implemented. When all this information is gathered together and evaluated with the MITRE ATT&CK matrix, the attack map of the APT group can be revealed.

Under the “Techniques” column, you can see what tools, software or techniques that the APT group was leveraged for the attack. For example, some software used by the “Lazarus Group” APT group is as in the image below:Software

Software are the programs developed to work on digital systems. In the software section of MITRE ATT&CK Framework, there are software used by APT groups.

Each software has a unique ID, name and description. For example, the below image shows the ID, Name and the Description of the software:

"3PARA RAT" software. The information on this page includes which techniques the software uses and which APT group(s) utilizes this

software.

There are quite a number of software included in the MITRE ATT&CK Framework and the names/IDs/Descriptions are constantly updated over time with the newly added software. The number of software at the time of preparation of this training is as follows:

Software - 718

EXPECTED OUTCOMES

Gain a thorough understanding of the MITRE ATT&CK Framework and its importance for SOC analysts.Develop knowledge of the various tactics, techniques, and procedures (TTPs) used by threat actors to conduct attacks on computer networks.Learn how to use the MITRE ATT&CK Framework to identify and categorize different types of attacks based on the tactics and techniques used.Understand how the MITRE ATT&CK Framework can be used to improve incident response and threat intelligence gathering.

.

What is the concept that expresses the motivation for the action of the cyber attacker within the MITRE ATT&CK Framework?

Tactic

Technique

Procedure

Mitigation

Conclusion:

The MITRE ATT&CK framework provides a matrix of tactics, techniques, and procedures (TTPs) used by cyber adversaries. While it's useful for detailing attacker behavior, it doesn't provide a linear progression of an attack.