MITRE ATT&CK FRAMEWORK

MITRE ATT&CK enables the grouping of steps and details to understand tactics and techniques used by cyber attackers. Its primary goal is to assist defense parties in dealing with cyber attacks more effectively.

Some concepts related to the MITRE ATT&CK framework:

• **Tactic:** Expresses the objective behind an attacker's target or actions.

• **Technique:** Represents the specific method or approach an attacker uses to achieve a tactical goal.

• **Procedure:** Represents the detailed implementation of a technique, covering specific steps taken by an attacker within a particular technique.

• **Mitigations:** Measures taken to prevent attacks.

• **Groups:** Communities conducting attacks. It defines specific attacker groups (APTs) and their tactics and techniques with examples.

• **Software:** Programs used to carry out attacks and detect and track tactics and techniques.

Key Stages: Tactics and Techniques

The MITRE ATT&CK framework classifies tactics according to different environments such as Enterprise, Mobile, and ICS. This report covers the most used Enterprise tactics with the highest number of techniques/sub-techniques. It defines the basic stages attackers follow during an attack, which include:

• **Reconnaissance:** Techniques where attackers gather information to carry out the attack.

• **Resource Development:** Techniques where attackers create resources for use during the attack.

• **Initial Access:** Techniques where attackers attempt to gain access to your network.

• **Execution:** Techniques where attackers attempt to run malicious software.

• **Persistence:** Techniques where attackers try to maintain access without disruption.

• **Privilege Escalation:** Techniques where attackers attempt to obtain higher-level access.

• **Defense Evasion:** Techniques where attackers try to avoid detection.

• **Credential Access:** Techniques where attackers attempt to access or manage user credentials.

• **Discovery:** Techniques where attackers gather information about systems and internal networks.

• **Lateral Movement:** Techniques where attackers attempt to access other systems within the network.

• **Collection:** Techniques where attackers gather necessary data as per their objective.

• **Command and Control:** Techniques where attackers communicate with and control the compromised system.

• **Exfiltration:** Techniques where attackers attempt to access targeted information and files.

• **Impact:** Techniques where attackers attempt to prevent access to or destroy your data.

Each stage is associated with various tactics and techniques. For example, under the "Initial Access (TA0001)" tactic, there are techniques such as "Phishing (T1566)" and "Drive-by Compromise (T1189)" while under the "Execution (TA0002)" tactic, the "Command and Scripting Interpreter (T1059)" technique includes sub-techniques like "PowerShell (T1059.001)."

These tactics and techniques are used to understand how attackers infiltrate target systems and execute attacks. Defense teams can focus on these tactics and techniques to develop strategies for detecting, preventing, and responding to attacks.