MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) is a framework containing information about various techniques and strategies used by adversaries. It is often used as a guideline or as a means of reference when evaluating the security posture of an organization. It is available to any person for free.

The framework mainly comprises tactics and techniques. Tactics refer to the common strategies which adversaries may use in achieving their goal. Examples of these include reconnaissance, persistence, defense evasion, etc. Techniques refer to the more specific methods adversaries may use to accomplish the strategy. For example, in privilege escalation, which is a tactic, adversaries may abuse privilege control mechanisms, or use access token manipulation, both of which are techniques which come under privilege escalation. Each technique can further be divided into sub-techniques.

Tactics, techniques and sub-techniques are appropriately labelled and given an identifier. For example, the tactic exfiltration has id TA0010. Automated exfiltration, which is a technique that comes under exfiltration, has the id T1020. Further, traffic duplication is a sub-technique of automated exfiltration and it has the id T1020.001. Each section contains further information regarding mitigation, real world usage etc.

Tactics and techniques can also differ depending on the type of system in question. One can find three further categories - Enterprise, Mobile and ICS, each listing out the tactics and techniques relevant to them. MITRE ATT&CK is also comprehensive because it includes information related to the type of environment too, be it containers, virtual machines or the cloud.

The MITRE ATT&CK matrix provides a clean and tabular form of tactics and techniques which can be easily understood. It is updated regularly to keep up with the constantly evolving strategies and methods.