What is Mitre Att&ck?

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 sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

What is in the MITRE ATT&CK Matrix?

The MITRE ATT&CK matrix contains a set of techniques used by adversaries to accomplish a specific objective. Those objectives are categorized as tactics in the ATT&CK Matrix. The objectives are presented linearly from the point of reconnaissance to the final goal of exfiltration or "impact". Looking at the broadest version of ATT&CK for Enterprise, which includes Windows, MacOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS, and Network environments, the following adversary tactics are categorized:

Reconnaissance:

gathering information to plan future adversary operations, i.e., information about the target organization

Resource Development:

establishing resources to support operations, i.e., setting up command and control infrastructure

Initial Access:

trying to get into your network, i.e., spear phishing

Execution:

trying the run malicious code, i.e., running a remote access tool

Persistence:

trying to maintain their foothold, i.e., changing configurations

Privilege Escalation:

trying to gain higher-level permissions, i.e., leveraging a vulnerability to elevate access

Defense Evasion:

trying to avoid being detected, i.e., using trusted processes to hide malware

Credential Access:

stealing accounts names and passwords, i.e., keylogging

Discovery:

trying to figure out your environment, i.e., exploring what they can control

Lateral Movement:

moving through your environment, i.e., using legitimate credentials to pivot through multiple systems

Collection:

gathering data of interest to the adversary goal, i.e., accessing data in cloud storage

Command and Control:

communicating with compromised systems to control them, i.e., mimicking normal web traffic to communicate with a victim network

Exfiltration:

stealing data, i.e., transfer data to cloud account

Impact:

manipulate, interrupt, or destroy systems and data, i.e., encrypting data with ransomware.


MITRE ATT&CK vs. CYBER KILL CHAIN
MITRE ATT&CK
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
Cyber Kill Chain
Reconnaissance
Intrusion
Exploitation
Privilege Escalation
Lateral Movement
Obfuscation/ Anti-forensics
Denial of Service
Exfiltration
VARONIS