Mitre Framework

- Knowledge base that describes the behaviors and tactics used by cyber attackers based on real-world observations.

- Resources used by cybersecurity professionals to understand, detect, analyze, and mitigate cyber threats.

- **MITRE Corporation** is a not-for-profit organization that works in the public interest across federal, state, and local governments, as well as industry and academia. It manages Federally Funded Research and Development Centers (FFRDCs).

MITRE ATT&CK stands for:

Adversarial Tactics, Techniques, and Common Knowledge

Purpose of MITRE ATT&CK

The MITRE ATT&CK framework helps:

- Detecting and responding to cyber threats more effectively.

- Understand attacker behavior patterns.

- Improve threat intelligence and incident response.

- Support red teaming, blue teaming, and purple teaming in cybersecurity.

Structure of MITRE ATT&CK

The framework is divided into several layers:

1. Tactics

- Definition: The "why" of an attack — the attacker’s goals or objectives.

- Examples:

    - Initial Access
    - Execution
    - Privilege Escalation
    - Defense Evasion
    - Credential Access
    - Discovery
    - Lateral Movement
    - Collection
    - Command and Control (C2)
    - Exfiltration
    - Impact

2. Techniques

- Definition: The "how" — specific ways attackers achieve the tactics.
- Examples:
    - Spearphishing Attachment (under Initial Access)
    - PowerShell (under Execution)
    - Credential Dumping (under Credential Access)

Each technique may also include:

- Sub-techniques: More detailed implementations of a technique.
- Detection methods
- Mitigations

3. Procedures

- Actual tools and behaviors used by threat actors, often mapped to known groups like APTs (Advanced Persistent Threats).

Types of ATT&CK Matrices

MITRE ATT&CK is divided into several **matrices**, depending on the environment:

Matrix	Description
Enterprise	Focuses on Windows, macOS, Linux, cloud, and network infrastructure.
Mobile	Focuses on attacks targeting mobile devices like Android and iOS.
ICS (Industrial Control Systems)	Covers threats to OT (Operational Technology) environments.

🔹 Tools Supporting ATT&CK

Many cybersecurity tools integrate MITRE ATT&CK, such as:

- **SIEMs** (e.g., Splunk, Elastic)
- **EDRs** (e.g., CrowdStrike, Microsoft Defender)
- **Threat intelligence platforms**
- **Purple Teaming platforms** (e.g., MITRE CALDERA, Atomic Red Team)