The **MITRE ATT&CK Framework** is a globally recognized knowledge base that describes the behavior and techniques used by cyber adversaries across different stages of an attack. It's widely used in cybersecurity for threat detection, incident response, and security assessments.

What It Is:

ATT&CK stands for **Adversarial Tactics, Techniques, and Common Knowledge**. It's essentially a **matrix** that maps out how attackers operate — from initial access to data exfiltration — based on real-world observations.

Key Components:

1. **Tactics** – The *why* of an attack (e.g., Initial Access, Execution, Persistence). These are the adversary's goals.
2. **Techniques** – The *how* (e.g., Phishing, PowerShell, Credential Dumping). These are specific methods used to achieve a tactic.
3. **Sub-techniques** – More detailed versions of techniques.
4. **Mitigations** – Defensive strategies to prevent or detect techniques.
5. **Detections** – Guidance on how to identify techniques in logs or telemetry.

Use Cases:

- **SOC Analysts** use it to map alerts to known attack behaviors.
- **Detection Engineers** use it to build and test detection rules.
- **Red Teams** use it to simulate real-world attacks.
- **Blue Teams** use it to improve defenses and visibility.

Example:

Tactic	**Technique**	**Sub-technique**
Initial Access	Phishing	Spear phishing Attachment
Execution	Command and Scripting	PowerShell

MITRE ATT&CK Matrix Overview

```
+---------------------+--------------------------+
|     Tactic          |       Techniques         |
+---------------------+--------------------------+
| Initial Access      | Phishing, Drive-by Compromise |
| Execution           | PowerShell, Scripting    |
| Persistence         | Registry Run Keys, Services  |
| Privilege Escalation| Exploitation for Privilege   |
| Defense Evasion     | Obfuscated Files, Masquerading|
| Credential Access   | Keylogging, Credential Dumping|
| Discovery           | System Info Discovery    |
| Lateral Movement    | Remote Desktop, SMB      |
| Collection          | Screen Capture, Clipboard    |
| Exfiltration        | Data Transfer to Cloud   |
| Command & Control   | Beaconing, DNS Tunneling     |
+---------------------+--------------------------+
```