MITRE

## 📓 **Notes – MITRE**

**Lab Name:** MITRE

**Summary:**  
The **MITRE Corporation** develops several important cybersecurity frameworks and resources used in SOC operations, threat intelligence, and defense planning. The most widely used is the **MITRE ATT&CK® Framework**, which provides a globally accessible knowledge base of adversary tactics and techniques.

### **Task 1 – Introduction to MITRE**

* MITRE is a non-profit that supports U.S. government R&D projects, including cybersecurity.
* Provides free, open frameworks like ATT&CK®, D3FEND, and Engage.

### **Task 2 – Basic Terminology**

* **Tactics** – The “why” behind attacker actions (high-level objectives).
* **Techniques** – The “how” — methods used to achieve tactics.
* **Sub-techniques** – More specific variations of techniques.
* **Procedures** – Detailed, real-world examples of attacker implementations.

### **Task 3 – ATT&CK® Framework**

* Categorized by **tactics** (columns) and **techniques** (rows).
* Covers different environments: **Enterprise**, **Mobile**, and **ICS**.
* Used for detection, threat hunting, incident response, and adversary emulation.

### **Task 4 – CAR Knowledge Base** (Cyber Analytics Repository)

* Provides analytics to detect adversary techniques.
* Maps analytics to ATT&CK tactics/techniques.
* Helps SOC teams build detections in SIEM/EDR.

### **Task 5 – MITRE Engage**

* Guidance for proactive defense and adversary engagement (deception, denial, and deterrence).

### **Task 6 – MITRE D3FEND**

* Companion to ATT&CK for defense.
* Lists countermeasures and security controls mapped to ATT&CK techniques.

### **Task 7 – ATT&CK® Emulation Plans**

* Step-by-step attacker behavior simulations for testing defenses.
* Useful for **purple teaming** (offense + defense collaboration).

### **Task 8 – ATT&CK® and Threat Intelligence**

* CTI teams map observed TTPs to ATT&CK techniques for standardized reporting.
* Helps share intel across organizations in a common format.

**Practical Takeaway:**

* ATT&CK is the **de facto standard** for SOC detection mapping and incident reporting.
* Combine ATT&CK + D3FEND for a full view of both attack and defense.
* Use CAR analytics to improve SIEM and EDR detections.

**Tools/Commands Used:**

* None — conceptual lab.

