**🔐 MITRE ATT&CK, Chain of Custody & Security Operations**

**Level:** Beginner-Friendly

**Domain:** Threat Intelligence, Incident Response, Cybersecurity Frameworks

**🧠 1. What is MITRE ATT&CK?**

**MITRE ATT&CK** stands for:

**Adversarial Tactics, Techniques, and Common Knowledge**

It’s like a **giant cheat sheet** of how real-world attackers operate, collected by MITRE (a non-profit R&D org in the U.S.).

**📊 Why Do We Use It?**

| **Purpose** | **Example** |
| --- | --- |
| Understand attacker behavior | How do hackers get in? What do they do next? |
| Build detection rules | Stop or alert on those behaviors |
| Perform threat hunting | Find hidden attackers inside networks |
| Simulate attacks | Red Team can follow real attacker steps |
| Train blue teams | Teach SOC analysts what to look for |

**🔍 Structure (Tactics → Techniques → Procedures)**

| **Term** | **Meaning** | **Example** |
| --- | --- | --- |
| **Tactic** | Goal of attacker | Persistence (stay inside system) |
| **Technique** | How goal is achieved | Create new admin account |
| **Procedure** | Real attack example | FancyBear created account svc-admin |

➡️ Each row in ATT&CK Matrix shows real hacker behavior  
Website: [https://attack.mitre.org](https://attack.mitre.org/)

**🧪 Example:**

**Tactic:** Initial Access

**Technique:** Phishing Email

**Procedure:** Hacker sends malicious Excel file with macro

**🧾 2. What is Chain of Custody?**

**Chain of Custody (CoC)** means keeping proper records when handling digital evidence — like a **crime scene log**.

**🧯 Why It’s Important:**

| **Why?** | **Explanation** |
| --- | --- |
| 🔐 Maintain evidence integrity | Nobody tampered with the data |
| 👩‍⚖️ Legal value | Admissible in court |
| 👨‍💻 Accountability | Know who accessed it and when |

**📋 What’s Included in Chain of Custody?**

1. **Where the evidence came from**

(e.g. Email server, USB drive, logs)

1. **Who collected it**

(Investigator name, timestamp)

1. **When and where it was stored**

(Location, sealing, hashes, etc.)

1. **Who accessed it?**

(Every time someone handled it)

**🔒 Real-Life Example:**

You found a suspicious file in a malware case.

✅ You log:

* Time collected: Aug 6, 2025, 10:35 AM
* By: Ahmad (SOC Analyst)
* File hash: sha256...
* Stored in: /forensics/evidence/case123/
* Accessed later by: Sarah (Malware Analyst)

**🧰 3. What is Security Operations (SecOps/SOC)?**

**Security Operations Center (SOC)** is a team and set of tools that **monitor and defend an organization 24/7**.

Think of it like a **cyber police station**.

**🛡️ What Do SOC Teams Do?**

| **Function** | **Example** |
| --- | --- |
| 🔍 Monitor logs & alerts | Firewall says port scanning detected |
| ⚠️ Detect attacks | SIEM shows login from foreign IP |
| 🚨 Incident response | Malware found → isolate machine |
| 📈 Threat hunting | Look for hidden attackers (proactive) |
| 🧪 Forensics | Analyze attack methods & root cause |
| 🎯 Reporting | Write post-incident reports & lessons learned |

**🧠 SOC Tools & Terms to Know**

| **Tool** | **Purpose** |
| --- | --- |
| **SIEM** (Splunk, ELK) | Log collection & alerting |
| **EDR** (CrowdStrike, SentinelOne) | Endpoint protection |
| **SOAR** | Automated response playbooks |
| **MITRE ATT&CK** | Mapping attacker behavior |
| **Case Management** | Track incident tickets |

**✅ Summary Table**

| **Concept** | **What it is** | **Why it matters** |
| --- | --- | --- |
| **MITRE ATT&CK** | Hacker behavior framework | Helps you understand & detect real attacks |
| **Chain of Custody** | Evidence handling log | Ensures trust, legality, and integrity |
| **Security Operations** | 24/7 cyber defense team | Detects, analyzes, and responds to threats |