Eviction

## 📓 **Notes – Eviction**

**Lab Name:** Eviction

**Summary:**  
The **Eviction** lab simulates the process of removing an active threat actor from an environment. It focuses on the **post-detection** phase, where a SOC analyst must coordinate with incident response (IR) teams to **contain, eradicate, and recover** from an intrusion without tipping off the attacker too early.

**Key Points Learned:**

* **Challenges of Eviction:**
  + If the attacker notices removal attempts, they may accelerate malicious actions.
  + Coordinated timing with all security teams is critical.
  + Multiple access points may exist — all must be removed simultaneously.
* **Phases of Eviction in IR:**
  + **Preparation:** Collect intelligence on attacker infrastructure and persistence methods.
  + **Planning:** Decide on a date/time for eviction with all stakeholders.
  + **Execution:** Remove malware, revoke credentials, block C2 infrastructure.
  + **Post-Eviction Monitoring:** Watch for signs of re-entry attempts.
* **Framework Mapping:**
  + **MITRE ATT&CK:** Focus on Persistence, Command & Control, and Defense Evasion tactics.
  + **Diamond Model:** Helps identify all attacker assets to remove during eviction.
* **Operational Security (OPSEC):**
  + Avoid changes that reveal detection before eviction date.
  + Maintain covert monitoring until the operation is ready.

**Practical Takeaway:**

* Eviction is not just technical — it requires **strategic planning** and **team coordination**.
* Best done as part of a **coordinated incident response plan**.

**Tools/Commands Used:**

* EDR console for isolation & malware removal
* SIEM queries for persistence detection

