# **Summit**

**📓 Notes – Summit**

**Lab Name:** Summit

**Summary:**  
This lab focuses on applying cyber defense frameworks in a practical SOC investigation scenario. The name "Summit" represents a simulated corporate environment where a potential cyber incident is unfolding, and the SOC analyst must analyze provided data to understand attacker behavior.

**Scenario Overview:**

* Organization detects suspicious network activity.
* SOC analyst tasked with applying frameworks like **Pyramid of Pain**, **Cyber Kill Chain**, and **MITRE ATT&CK** to categorize and track the intrusion.

**Key Points Learned:**

* **Framework Integration:**
  + Use the **Cyber Kill Chain** to identify where in the attack sequence the detection occurred.
  + Map observed activity to **MITRE ATT&CK tactics/techniques** for clarity and standardization.
  + Assess impact using the **Diamond Model** (Adversary, Capability, Infrastructure, Victim).
* **Threat Intelligence Usage:**
  + Identify IOCs (IPs, domains, hashes) and map them to Pyramid of Pain categories.
  + Consider the longevity and disruption impact of each IOC type.
* **SOC Workflow Highlighted:**
  + Alert triage
  + Evidence gathering
  + Framework mapping
  + Decision-making (escalate or close case)

**Practical Takeaway:**

* Using multiple frameworks together provides a **360-degree view** of the attack.
* Even without full details, partial IOC mapping can still be valuable for early detection.
* Documentation is critical — record all findings in a SOC case ticket.

**Tools/Commands Used:**

* SIEM dashboard queries
* IOC lookup in threat intel databases

