OpenCTI

## 📓 **Notes – OpenCTI**

**Lab Name:** OpenCTI

**Summary:**  
**OpenCTI** (Open Cyber Threat Intelligence) is an open-source threat intelligence platform designed to **structure, store, organize, and visualize** cyber threat knowledge.  
It integrates with multiple intel sources and supports collaborative CTI work for SOC, IR, and Threat Hunting teams.

### **Task 1 – Room Overview**

* Purpose: Learn how to use OpenCTI for threat intelligence management and investigations.

### **Task 2 – Introduction to OpenCTI**

* Free and open-source TIP (Threat Intelligence Platform).
* Uses **STIX 2.1** (Structured Threat Information Expression) to standardize intel data.
* Can ingest intel from MISP, AlienVault OTX, Abuse.ch, and other sources.

### **Task 3 – OpenCTI Data Model**

* Core concepts:
  + **Entities:** Threat actors, malware, vulnerabilities, tools, etc.
  + **Relationships:** How entities are connected (e.g., malware used by threat actor).
  + **Observables:** Raw IOCs (IP, domain, hash, URL).
* Enables rich link analysis between threats.

### **Task 4 – OpenCTI Dashboard 1**

* Overview dashboard shows **threat actors, malware families, campaigns, intrusion sets**.
* Filter and search for specific intelligence data.

### **Task 5 – OpenCTI Dashboard 2**

* Relationship view: See connections between threat actors, campaigns, and IOCs.
* Timeline view: Track when certain indicators or activities were observed.

### **Task 6 – Investigative Scenario**

* Scenario: An alert from the SOC leads to OpenCTI search.
* Steps:
  1. Lookup an IOC in OpenCTI.
  2. See related malware, threat actors, and campaigns.
  3. Use this context to update SOC case and improve detection rules.

### **Task 7 – Room Conclusion**

* OpenCTI helps analysts move beyond raw IOCs to **context-rich intelligence**.
* Facilitates correlation across multiple data sources.
* Improves threat hunting and incident response efficiency.

**Practical Takeaway:**

* OpenCTI is a central hub for **linking threats, actors, and IOCs**.
* Visualization helps analysts quickly understand complex relationships.
* Works best when fed with automated data ingestion from multiple feeds.

**Tools/Commands Used:**

* OpenCTI Web UI (search, filters, graph view).

