MISP

## 📓 **Notes – MISP**

**Lab Name:** MISP (Malware Information Sharing Platform)

**Summary:**  
**MISP** is an open-source Threat Intelligence Platform (TIP) that enables organizations to **collect, store, share, and correlate cyber threat intelligence**.  
It’s a key tool in SOC and Incident Response workflows for sharing structured threat data in real-time.

### **Task 1 – Room Overview**

* Goal: Learn core MISP functions, features, and how to use it for collaborative threat intelligence.

### **Task 2 – MISP Introduction: Features & Terminologies**

* **Features:**
  + IOC sharing and correlation.
  + Support for **STIX, OpenIOC, CSV** formats.
  + Feeds and automated data ingestion.
  + Visualization of threat relationships.
* **Key Terminology:**
  + **Event:** A collection of IOCs and related intelligence.
  + **Attribute:** Individual IOC (IP, domain, hash, etc.).
  + **Tag/Taxonomy:** Labels applied for categorization (e.g., TLP:AMBER).
  + **Galaxy:** Predefined knowledge sets (e.g., threat actor profiles).

### **Task 3 – Using the System**

* Main dashboard allows browsing, searching, and creating events.
* Adding an event involves:
  1. Title and description.
  2. Adding IOCs as attributes.
  3. Tagging with taxonomies and galaxies.
* Events can be shared with specific organizations or communities.

### **Task 4 – Feeds & Taxonomies**

* **Feeds:** Automated imports of intel from trusted sources (e.g., CIRCL, Abuse.ch).
* **Taxonomies:** Structured tagging systems (TLP, ATT&CK mappings).
* Feeds can auto-populate events or enrich existing ones.

### **Task 5 – Scenario Event**

* Example: SOC analyst receives a malicious domain from an alert.
* Steps in MISP:
  + Search domain in MISP.
  + See related events and attributes.
  + Correlate with malware families, threat actors, and campaigns.
  + Share findings with partner organizations.

### **Task 6 – Conclusion**

* MISP enhances collaboration and speeds up IOC correlation.
* Helps SOC teams go beyond isolated incidents to recognize broader campaigns.
* Works best with regular feed updates and integration with SIEM/IR tools.

**Practical Takeaway:**

* MISP is not just a database — it’s a **collaboration platform** for cyber defense.
* Strong integration with MITRE ATT&CK, OpenCTI, and automated feeds makes it powerful for SOC workflows.

**Tools/Commands Used:**

* MISP Web UI (event creation, IOC search, feed management).

