Threat Intelligence Tools

## 📓 **Notes – Threat Intelligence Tools**

**Lab Name:** Threat Intelligence Tools

**Summary:**  
This lab introduces several tools used in **Cyber Threat Intelligence (CTI)** to collect, analyze, and share information about adversaries, campaigns, and Indicators of Compromise (IOCs).  
SOC analysts use these tools to enrich alerts, validate suspicious activity, and understand attacker tactics.

**Key Points Learned:**

### **1. IOC Lookup & Analysis Tools**

* **VirusTotal** – Aggregates antivirus and sandbox results for files, URLs, domains, IPs.
* **Hybrid Analysis** – Online sandbox for dynamic malware analysis.
* **Any.Run** – Interactive malware sandbox.

### **2. Threat Intelligence Platforms (TIPs)**

* **MISP (Malware Information Sharing Platform)** – Open-source TIP for storing and sharing threat intel.
* **OpenCTI** – Graph-based threat intel management.

### **3. Threat Feeds & OSINT Tools**

* **AlienVault OTX** – Free platform for sharing and consuming threat indicators.
* **Abuse.ch Feeds** – Specialized malware & botnet tracking (e.g., URLhaus, Feodo Tracker).
* **CIRCL Passive DNS** – Look up DNS history for domains/IPs.

### **4. Automation & Enrichment Tools**

* **TheHive** – Incident response platform with intel integration.
* **Cortex** – Analysis and enrichment engine that works with TheHive.

**SOC Workflow Integration:**

* Receive SIEM alert → Extract IOC → Lookup in multiple threat intel sources → Enrich case with findings → Decide on escalation or closure.

**Practical Takeaway:**

* No single tool covers all needs — analysts combine feeds, TIPs, and sandboxes.
* Enrichment context speeds up decision-making and reduces false positives.

**Tools/Commands Used:**

* Web interfaces of VirusTotal, Hybrid Analysis, MISP, AlienVault OTX.

