Trooper

## 📓 **Notes – Trooper**

**Lab Name:** Trooper  
**Category:** Cyber Threat Intelligence – Notes

### **Summary:**

**Trooper** is a hands-on threat intelligence analysis exercise where you work as a SOC analyst to investigate suspicious activities and uncover the details of a cyberattack using **threat intelligence tools**.  
The lab focuses on **gathering, correlating, and enriching IOCs** from various sources to build a clear picture of an adversary’s TTPs (Tactics, Techniques, and Procedures).

### **Key Learnings from Lab:**

#### **1. Investigating Initial Indicators**

* Started with a suspicious domain flagged by the SIEM.
* Looked up the domain in **threat intel platforms** (MISP, OpenCTI, VirusTotal, URLhaus).
* Found related malicious IPs, file hashes, and campaign details.

#### **2. IOC Correlation**

* Connected indicators across **different datasets**.
* Learned to pivot from one IOC to related infrastructure (shared IP hosting, DNS records, SSL certs).

#### **3. Attribution Steps**

* Linked the activity to a known threat actor profile in MITRE ATT&CK database.
* Used ATT&CK techniques to map the observed behavior.

#### **4. Enrichment & Prioritization**

* Classified IOCs by confidence level (high, medium, low).
* Prioritized response actions based on the severity and active status of the indicators.

### **Practical Takeaways:**

* Combining multiple intel sources provides a **complete picture** of a threat.
* IOC context is critical for making informed response decisions.
* SOC analysts should not rely on a single feed — cross-verification is essential.

**Tools Used:**

* MISP
* OpenCTI
* VirusTotal
* URLhaus
* MITRE ATT&CK Navigator

