## **Interview Project: Threat Intelligence Automation**

**To Note**: This project should be completed and submitted within 24 hours.

### **Objective**

The candidate must develop a Python security analysis tool that:

* Extract and analyze PCAP network traffic for suspicious activity.
* Parses network traffic to detect threats.
* Correlates logs with at least three Threat Intelligence Feeds.

### **Tasks**

1. **Network Analysis (30%)**: Extract key fields or metadata from the packet dump.
   1. Source & Destination IPs
   2. Protocols (TCP, UDP, HTTP, DNS)
   3. Suspicious User-Agent Strings
   4. Files and File signatures
2. **Threat Detection (20%)**: Identify malicious requests from the logs.
3. **Threat Intelligence Correlation (20%)**: Compare key fields from the PCAP files against three threat feeds.
4. **Reporting (20%)**: Generate a detailed Markdown security report:
   1. **Log-based threats**.
   2. **PCAP-based threats**.
   3. **Threat intelligence matches**.

## **Expected Deliverables**

* **GitHub Link**
* **Python script**
* **PCAP file**
* **Generated security report (security\_report.md)**: It should include the following:
  + Introduction
  + Scope and objective
  + Findings and recommendations
  + References: A list of all the threat intelligence feeds that were used
  + Conclusion
* **README.md** (execution instructions).

## **Sample PCAP Files**

* **Sample PCAPs**: <https://www.malware-traffic-analysis.net/>