Industrial IoT Honeypot and Threat Enrichment Pipeline

Project Report

Course: INDUSTRIAL IOT – University of Messina

Instructor: Prof. Giovanni Merlino

Student: Rana Sanjideh

July 3, 2025

1. Project Summary

This project simulates an Industrial Control System (ICS) environment to detect and analyze cyber threats. It deploys a Modbus honeypot, collects suspicious traffic, enriches it with threat intelligence, and visualizes results using a modern observability stack.

2. System Architecture

2.1. Components and Roles

Component	**Purpose**
Conpot	Honeypot that simulates a Modbus industrial device
Suricata	Network IDS that logs events as structured JSON
Logstash	Processes and enriches logs with threat data
Elasticsearch	Stores and indexes enriched logs
Kibana	Visualizes logs via real-time dashboards

3. Data Pipeline Flow

1. **Conpot** listens on port 502 to attract Modbus scans.
2. **Suricata** monitors traffic and logs events to `eve.json`.
3. **Logstash** enriches logs with:
   - GeoIP location
   - ASN information
   - AbuseIPDB threat score
   - Tags like `threat_match`, `private_ip`
4. **Elasticsearch** stores enriched logs.
5. **Kibana** visualizes attacker behavior and network threats.

4. Testing Methodology

Attacks are simulated using tools such as:

- **Nmap:** `nmap -Pn -sV -p 502 --script modbus-discover localhost`
- **Modpoll:** Dockerized client with CSV configuration

Logs are monitored via Docker containers:

- `docker logs -f conpot`
- `docker logs -f suricata`
- `docker logs -f logstash`

5. Kibana Visualizations

Dashboards include:

- Top attacker IPs by threat score
- Geolocation heatmaps
- Timeline of Modbus scans
- Tagged events such as `threat_match`

6. Sample Enriched Fields

- `source.ip`
- `geoip.country_name`
- `abuseConfidenceScore`
- `tags`
- `asn.organization`

7. Outcomes

- Real-time detection of Modbus scans
- Enriched data for deeper threat analysis
- Interactive dashboards via Kibana
- Foundation for scalable threat hunting

8. Future Improvements

- Add support for additional honeypot protocols (BACnet, FTP, etc.)
- Set up alerting and notifications
- Integrate external threat feeds (AlienVault, OTX)
- Package project for educational or portfolio showcase