IoT Honeypot with Threat Intelligence Integration

IOT Project
UNIME Department of Engineering
Professor Giovanni Merlino
Student Rana Sanjideh

STVDIORVM VNIVERSITAS MESSANAE
A.D.1548

Summery

This project develops a modular, containerized honeypot environment simulating ICS/SCADA networks. It captures real-world cyberattacks, enriches captured telemetry with threat intelligence, validates detection coverage through attack simulations, and introduces novel fingerprinting techniques for attacker attribution.

Concepts

- Deploy scalable honeypots using Docker Compose / K3s.

- Simulate ICS targets using Conpot and test with MITRE Caldera.

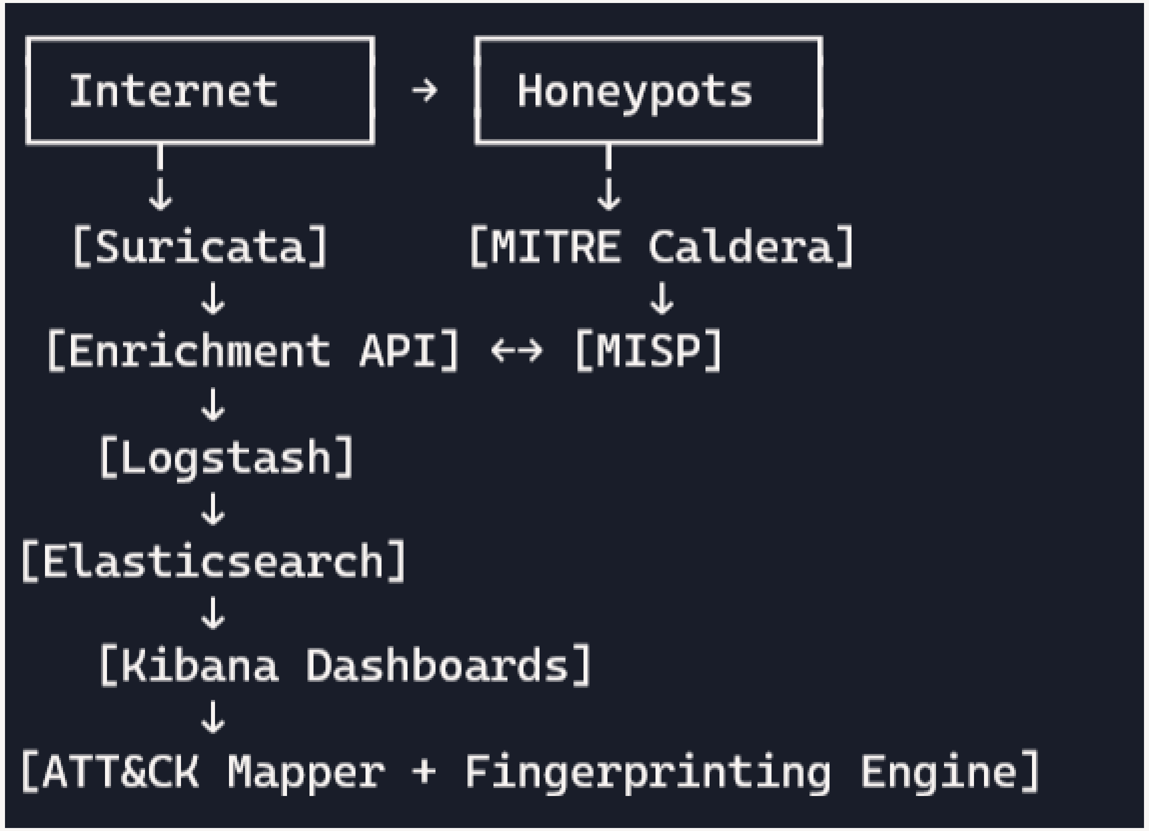
- Analyze enriched telemetry via ELK Stack + Suricata/Zeek.

- Automate mapping to MITRE ATT&CK.

- Correlate data with MISP for contextualized threat intelligence.

- Innovate with real-time fingerprinting of attacker tools and devices

Architecture



```
┌──────────────┐   ┌──────────────┐
│  Internet    │ → │  Honeypots   │
└─────┬────────┘   └─────┬────────┘
      ↓                  ↓
  [Suricata]      [MITRE Caldera]
        ↓                 ↓
 [Enrichment API] ↔ [MISP]
        ↓
   [Logstash]
        ↓
[Elasticsearch]
        ↓
   [Kibana Dashboards]
        ↓
[ATT&CK Mapper + Fingerprinting Engine]
```

Technical Modules

- Containerized Services:
- Conpot, Logstash, Elasticsearch, Kibana
- Suricata, Enrichment API, ATT&CK mapper
- Managed via: Docker Compose (dev), K3s/K3d (test/prod)
- Benefits:
- Rapid reusability
- Cloud/on-prem deployment flexibility
- Simplified CI/CD and integration testin

Threat Visibility Enhancements

- Data Enrichment Microservice:
- Geolocation (MaxMind)
- ASN and domain info
- Reputation data (AbuseIPDB, OTX)
- Output: Highly contextualized logs for enhanced analysis and pivoting in dashboards

Simulated Attack Validation

- Tool: MITRE Caldera
- Agents simulate full attack chains mapped to ATT&CK matrix
- Validates detection coverage and visual mapping accuracy
- Identifies gaps in visibility for further improvement

Threat Correlation with MISP

- Bidirectional Integration:

- Push enriched IOCs to MISP for sharing
- Pull threat intel (IP, hashes, JA3) to correlate with local findings

- Benefits:

- Attribution support
- Real-time enrichment loop
- Enhanced threat landscape awareness

Fingerprinting Innovation

- TCP/IP behavior + JA3/JA3S TLS signatures
- Timing anomalies, protocol misuses
- Clustering by entropy of headers, session duration
- Exportable feature sets for machine learning

Deliverables

- Fully operational Conpot honeypot infrastructure.
- Centralized log collection, analysis, and alerting via ELK.
- MITRE ATT&CK alignment for all logged incidents.
- A fingerprinting database/toolkit for adversary behavior.
- Research paper and/or GitHub repo showcasing methods and findings.

Expected Outcomes

- Production-ready honeypot infrastructure
- End-to-end enriched telemetry & mapping
- Real-world validated detection coverage
- New fingerprinting datasets
- Threat intelligence feeds and research output

Thank you

Rana Sanjideh

RanaSanjideh@gmail.com

DIPARTIMENTO INGEGNERIA
UniMe