

IoT-Vigilance

Vigilance on IT and OT asset security and resilience

G. Agosta³, P. Belluco⁴, L. Bozzi⁵, A. Campi³, F. Di Battista², L. Di Nicola¹

¹Go-Infoteam, Pescara, Italy; ²Project Innovation, L'Aquila, Italy; ³Politecnico di Milano, Milan, Italy; ⁴LWT3, Milan, Italy; ⁵SeaSkyTechnologies, Rome, Italy

Objectives

Asset Management

- Inventory ICT infrastructure
- Analyze interdependencies

Vulnerability Management

- Identify vulnerabilities
- Mitigate risks

Needs and Motivations

Infrastructure Knowledge

- Document ICT assets

Proactive Security

- Early vulnerability detection
- Mitigation strategies

OT Security Extension

- Include OT devices in analysis

Implementation Challenges

Framework Complexity

- Navigating complex frameworks

IT/OT Convergence

- Managing different protocols

Legacy Systems Integration

- Compatibility issues

Penetration Testing for OT

- Ensuring safety and reliability

Resource Constraints

- Budget limitations
- Skilled workforce shortage

Fuzzing and Malformed Input Testing

- Inventory ICT infrastructure
- Analyze interdependencies

Needs and Motivations

Integration of IT and OT Security

- Comprehensive IT/OT solution

Automated Penetration Testing for OT

- Addresses market gap

Conclusion

- Unified tool for ICT security
- Addresses IT and OT needs
- Leverages emerging trends
- Effective cybersecurity solution

Legacy Systems Integration

- Compatibility issues

Emerging Trends and Solutions

IT/OT Convergence

- **Solution:** Unified platform for IT and OT

NIS 2 Directive Compliance

- **Solution:** Stringent security measures

Automation and AI

- **Solution:** Machine Learning for automated detection

IoT Device Security

- **Solution:** Security analysis for IoT devices

Increase in OT Attacks

- **Solution:** Automated Penetration Testing for OT

Fuzzing Technologies

- **Solution:** Identify vulnerabilities in OT protocols

The IoT-Vigilance Solution

Asset Management

Inventory Smart Meters
Analyze Dependencies



Risk Mitigation

Patch Management
Configuration Updates



Continuous Monitoring

Real-time Alerts
Periodic Reports



Penetration Testing

Fuzzing Techniques
Malformed Input Testing



Vulnerability Assessment

Automated Scanning
Manual Analysis

Asset & Vulnerability Management Software Frontend

Interface TCP/IP

OT BOX

Protocols (DLMS)

SM

BASED ON REST API

- Starts, pauses, and stops scanning
- Identifies the object to be scanned (asset)
- Receives from the proxy and historizes the data from the scan
- Shows the output to the user

REST API BASED API

- Translates data from REST API to DLMS and vice versa

- It performs tests by "sending to" and "receiving data from the" OT device

- It performs tests by "sending to" and "receiving data from the" OT device

STAGE 1 ARCHITECTURE:

The flow allows you to run preset tests and historicize the commands executed in testing and the raw responses received

STAGE 2 (next step):

Add interpretation of received data to allow output to the user and add machine learning as a module to scan control and/or analysis of the results.