IoT-Vigilance

Vigilance on IT and OT asset security and resilience

G. Agosta[3], P. Belluco[4], L. Bozzi[5], A. Campi[3], F. Di Battista[2], L. Di Nicola[1]

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

Objectives

Asset Management

- Inventory ICT infrastructure
- Analyze interdependencies

Vulnerability Management

- Identify vulnerabilities
- Mitigate risks

Needs and Motivations

Infrastructure Knowledge

- Document ICT assets

OT Security Extension

- Include OT devices in analysis

Proactive Security

- Early vulnerability detection
- Mitigation strategies

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

Legacy Systems Integration

- Compatibility issues

Conclusion

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

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

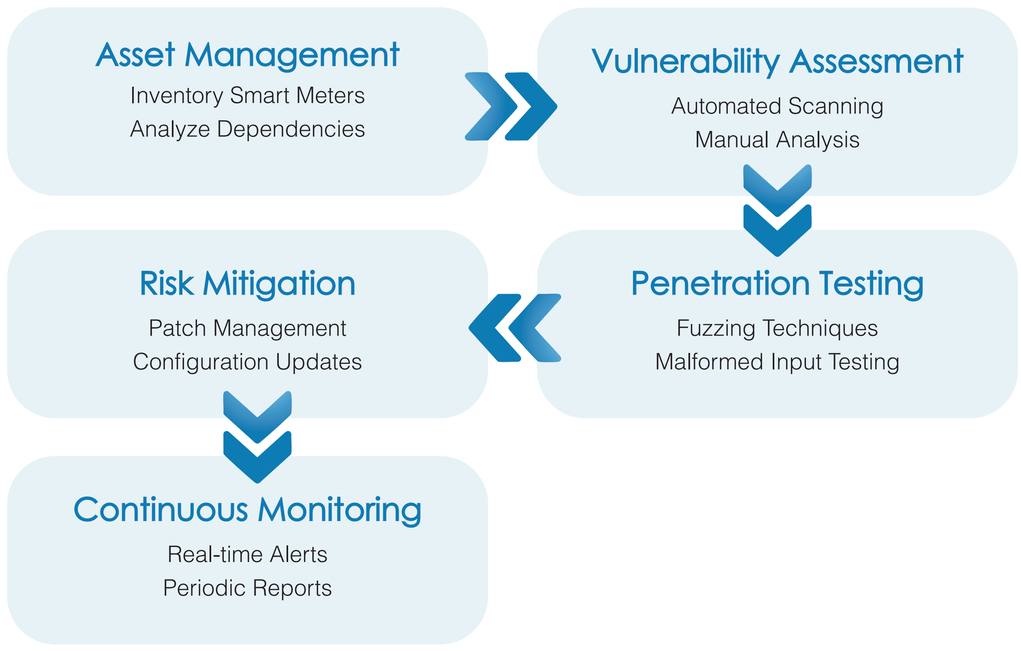
Increase in OT Attacks

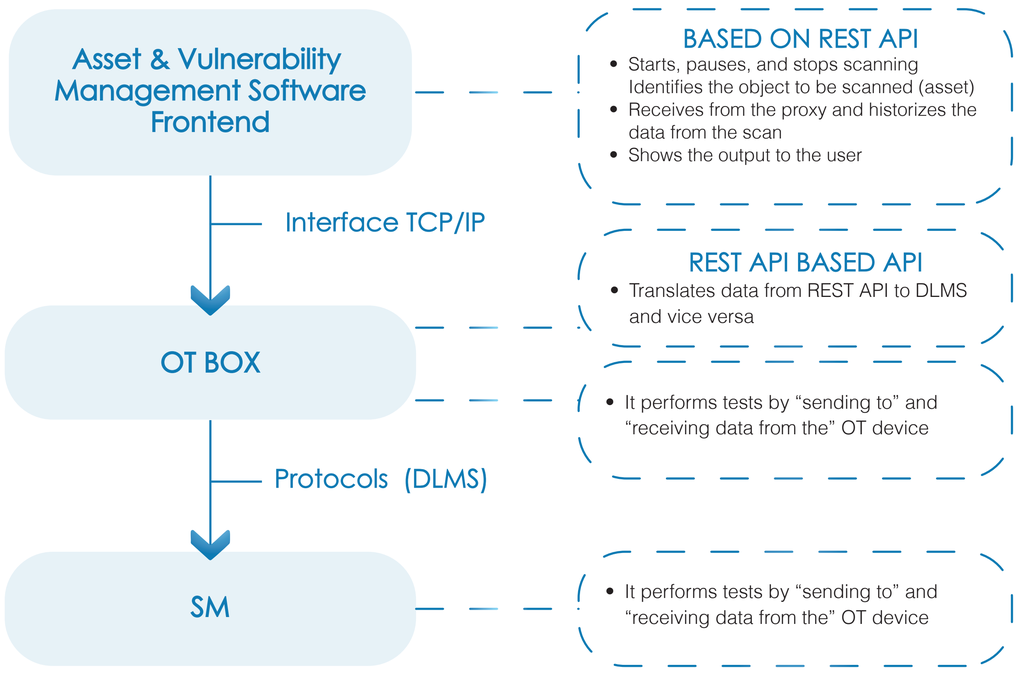
- **Solution:** Automated Penetration Testing for OT

Fuzzing Technologies

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

The IoT-Vigilance Solution





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.

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

VITALITY