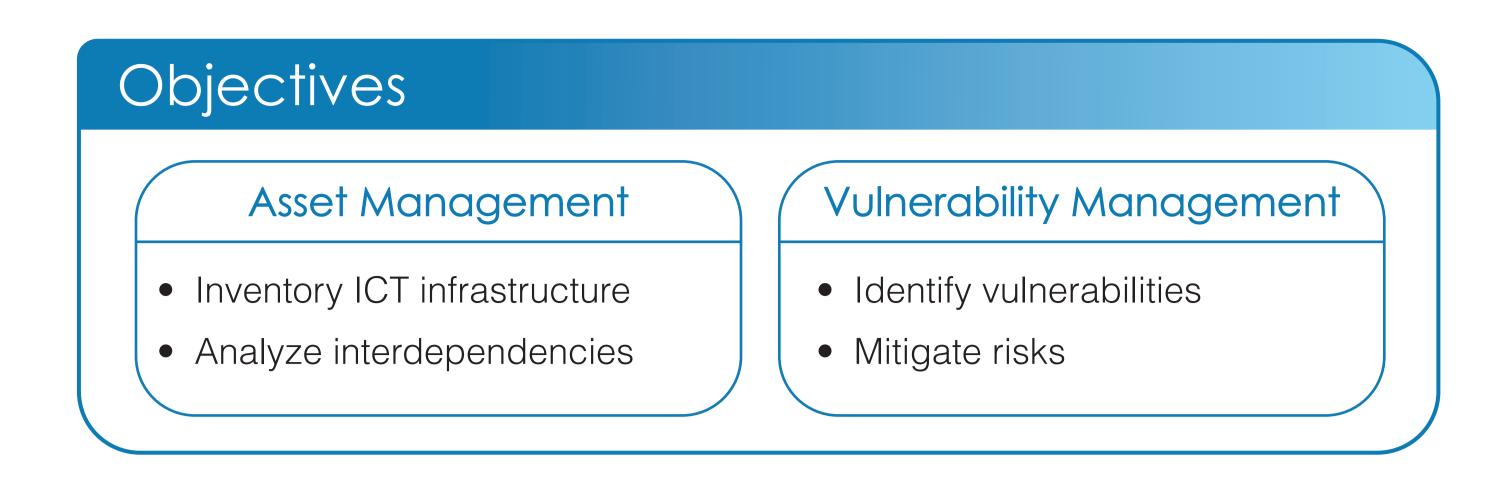


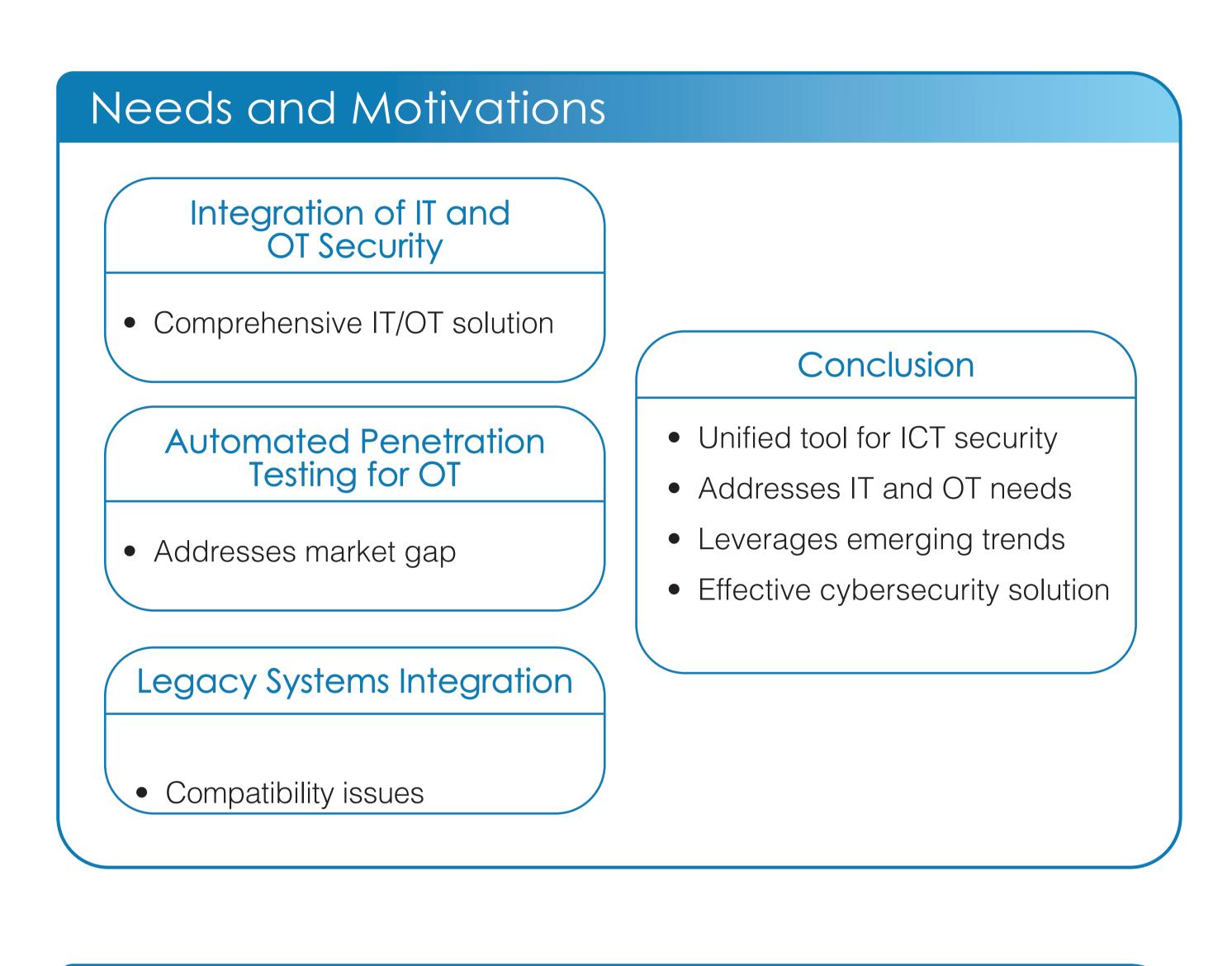
Vigilance on IT and OT asset security and resilience

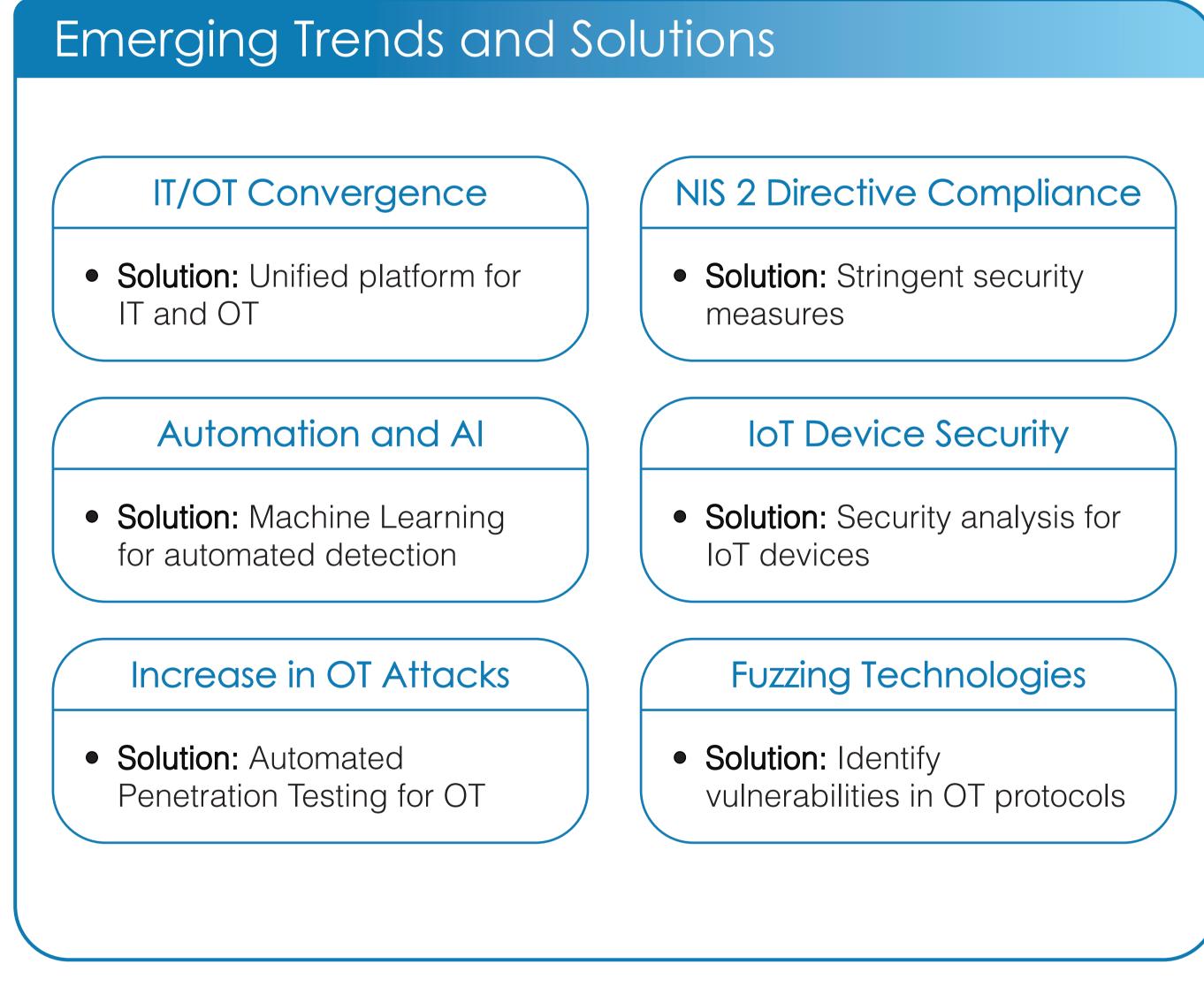
G. Agosta³, P. Belluco⁴, L. Bozzi⁵, A. Campi³, F. Di Battista², L. Di Nicola¹ ¹Go-Infoteam, Pescara, Italy; ²Project Innovation, L'Aquila, Italy; ³Politecnico di Milano, Milan, Italy; ⁴LWT3, Milan, Italy; ⁵SeaSkyTechnologies, Rome, Italy



Needs and Motivations Infrastructure Knowledge Proactive Security Document ICT assets Early vulnerability detection OT Security Extension Mitigation strategies Include OT devices in analysis

Implementation Challenges Framework Complexity IT/OT Convergence Navigating complex frameworks Managing different protocols Legacy Systems Integration Penetration Testing for OT Compatibility issues Ensuring safety and reliability Fuzzing and Malformed Input Testing Resource Constraints Budget limitations Inventory ICT infrastructure Skilled workforce shortage Analyze interdependencies





The IoT-Vigilance Solution

Asset Management

Inventory Smart Meters Analyze Dependencies



Risk Mitigation

Patch Management Configuration Updates



Continuous Monitoring

Real-time Alerts Periodic Reports



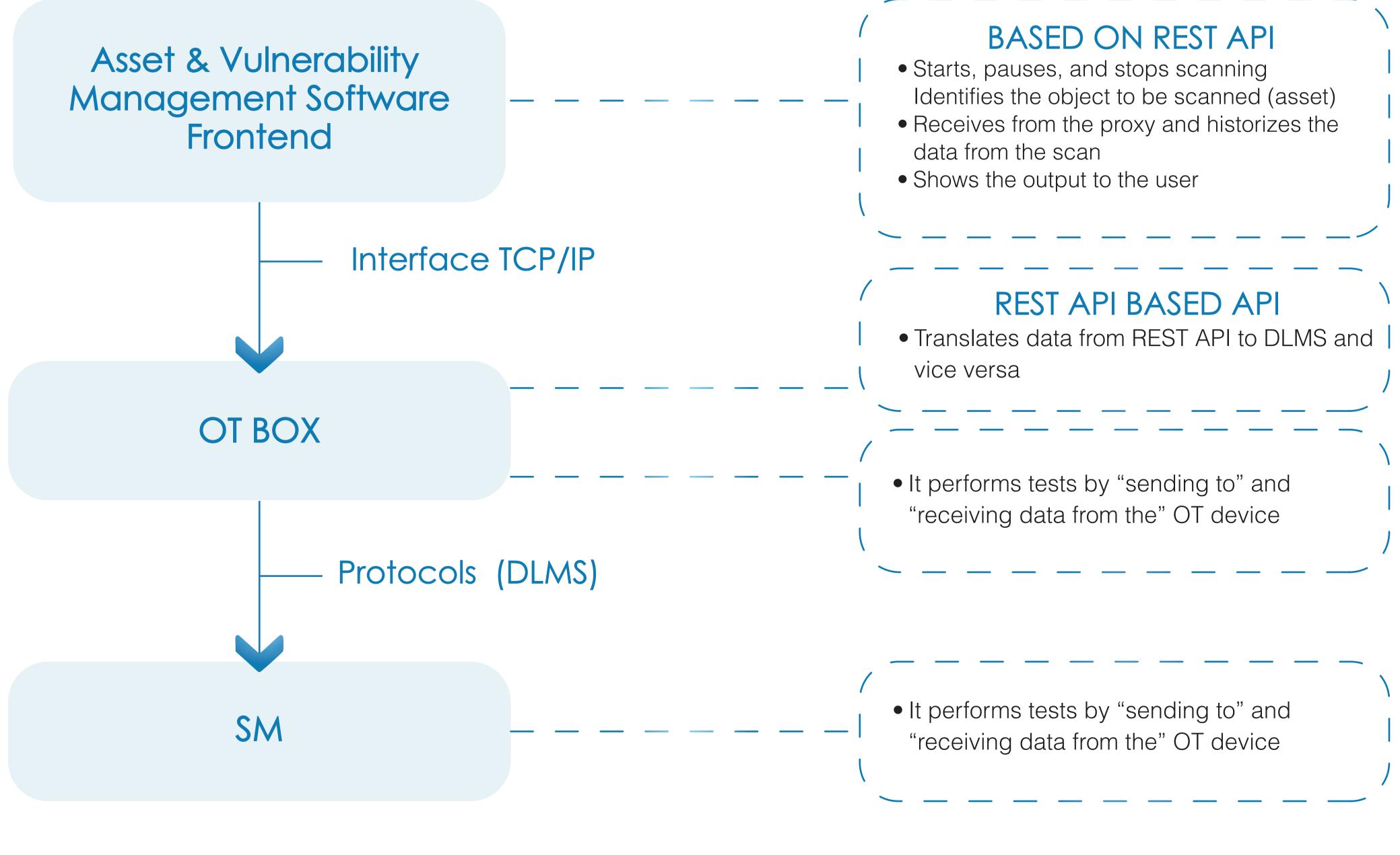
Penetration Testing

Fuzzing Techniques Malformed Input Testing



Vulnerability Assessment

Automated Scanning Manual Analysis



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.













