This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

A Multi-Level Approach to Resilience of Critical Infrastructures and Services

Antonios Gouglidis

2nd HyRiM End User Workshop
Barcelona, 15.11.2016

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

Contents

- Motivation
- Resilience
- Proposed architecture
- Evaluation results
- Concluding remarks

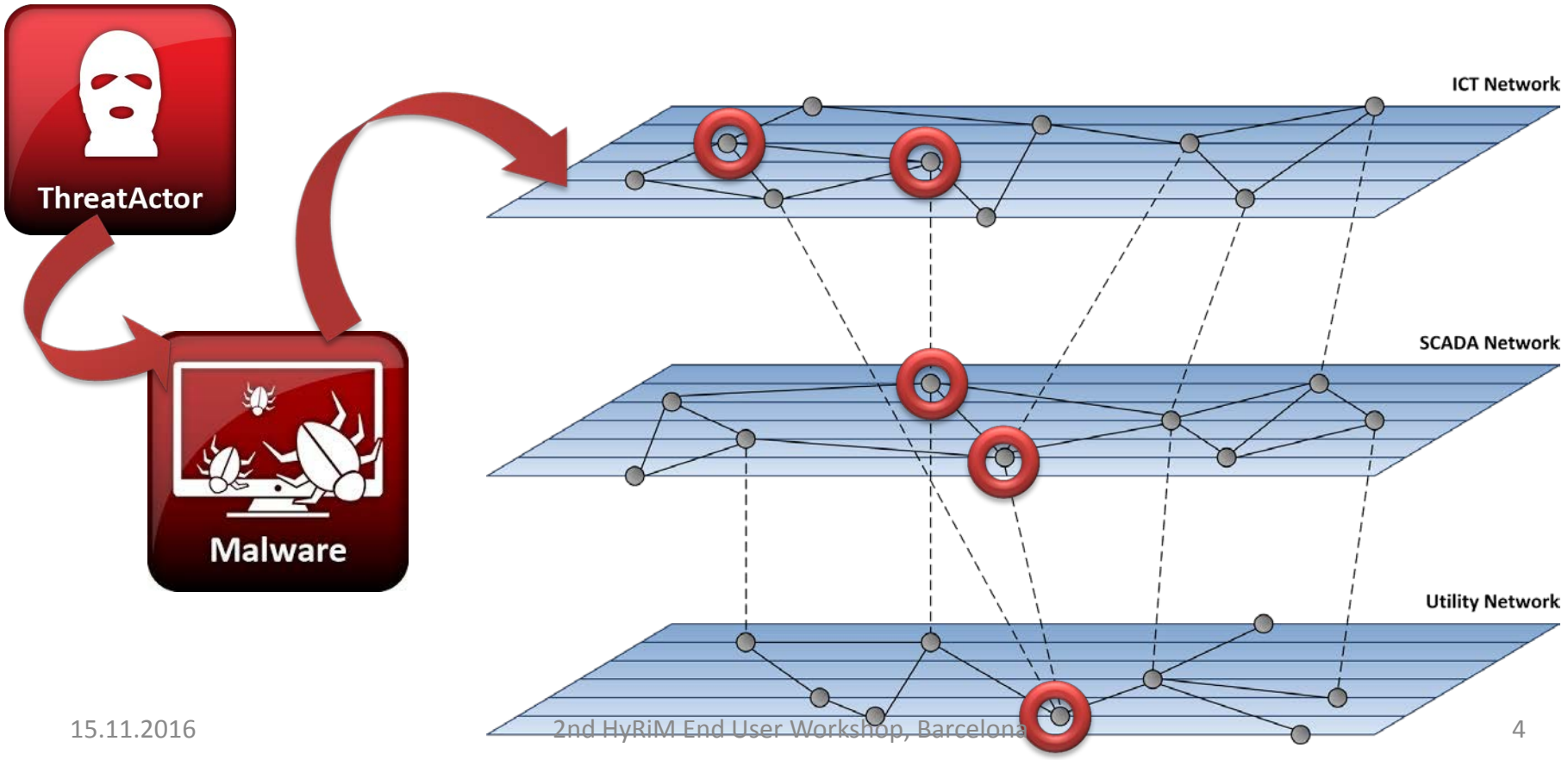
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Motivation

- Protection of Critical Infrastructures
- Threats on the rise – Serious cyber attack believed likely
- Investigate threats
- Provide foundations
  - Novel protection mechanisms

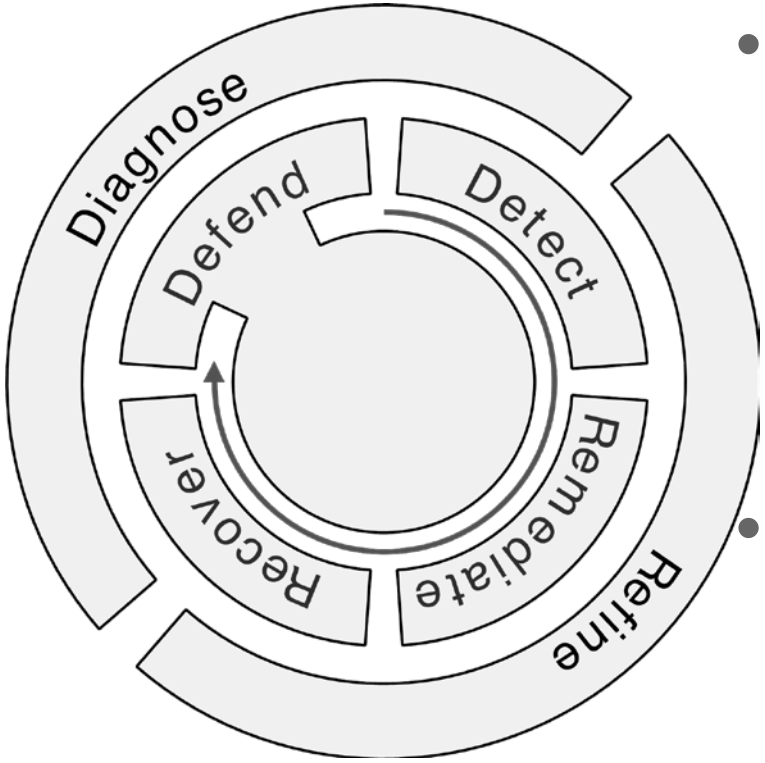
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

… a typical attack …



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Resilience and ways of achieving it…



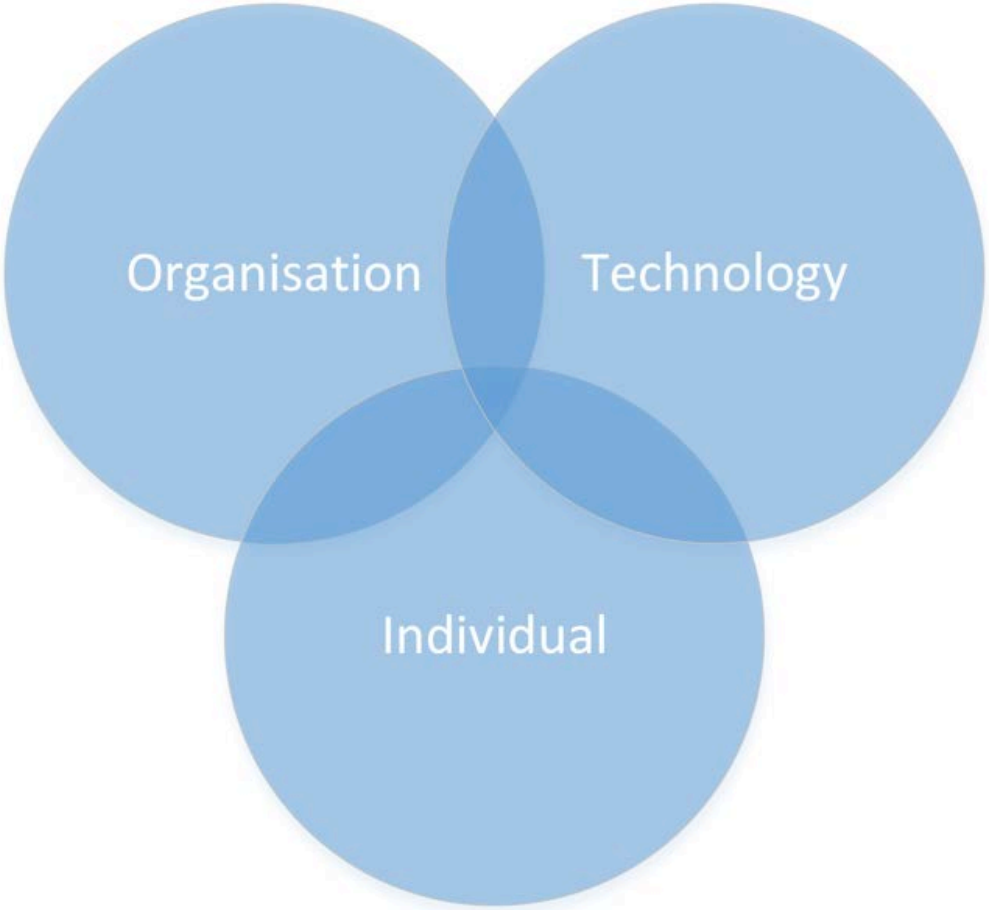
Resilience strategy

- *'… the ability of a network/system to defend against and maintain an acceptable level of service in the presence of challenges.' **
- D^2R^2+DR
  - Real-time control (internal) loop
  - Background (external) loop

* Sterbenz, James PG, et al. "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines." Computer Networks 54.8 (2010): 1245-1265.

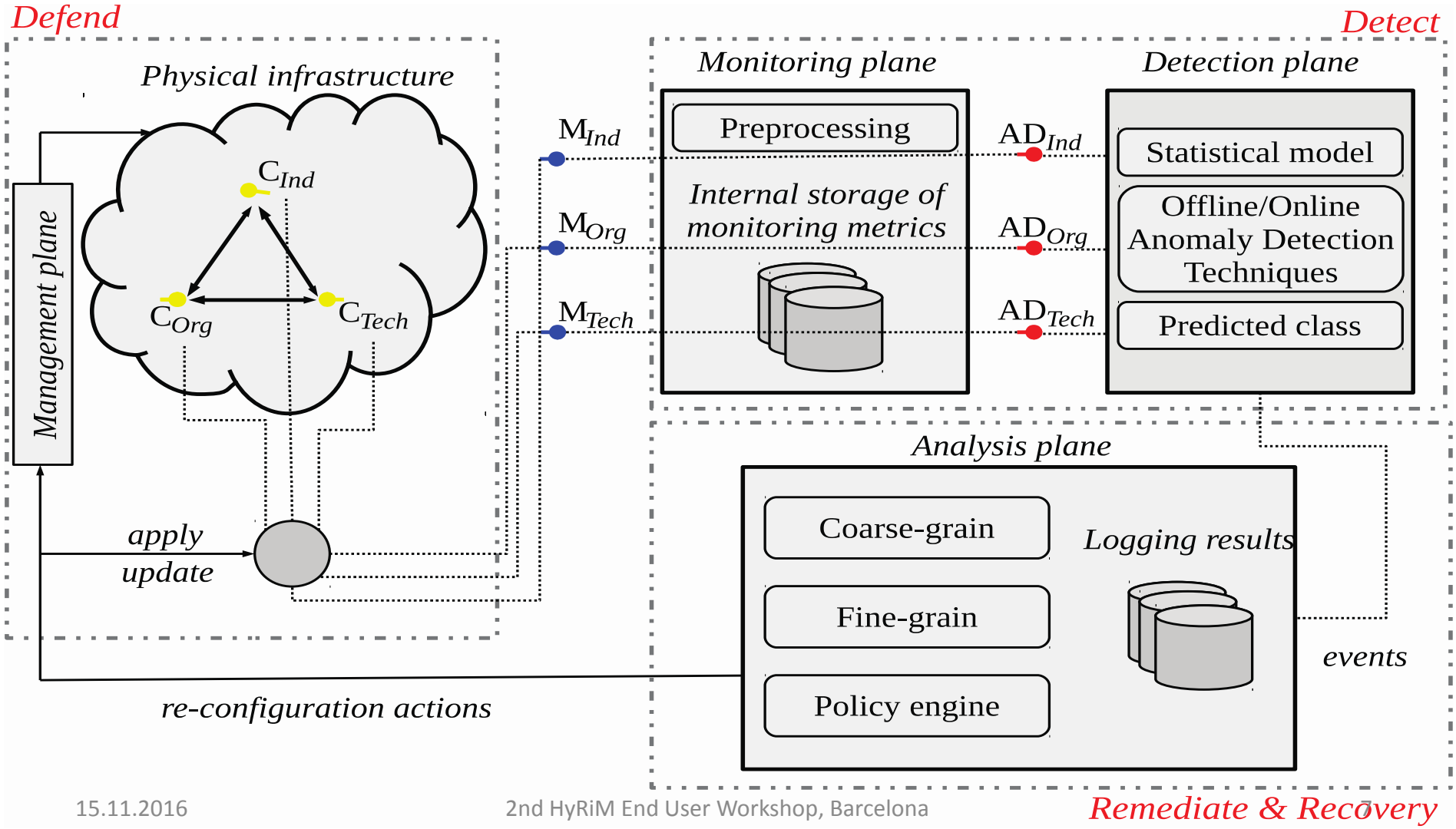
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

Viewpoints for utility networks



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

Resilience architecture



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

What metrics to measure?

HyRiM

- Periodic: Measure security control maturity and performance
  - E.g., Percentage of applications and systems subject to security testing
  - Challenge: High-level with long-term validation requirements
- Real-Time: Provide indicators of real-time threats
  - E.g., number of un-authorised access attempts, network throughput
  - Challenge: Conversion of measurements to representative metrics

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Examples of Threats and Metrics

HyRiM

Threat	Metrics	OTI Level	Collector
BYOD	No. of connected personal devices No. of invalid running applications	Organisation Individual	C_{Org} C_{Ind}
Remote Access	No. of active remote connections	Organisation	C_{Org}
Spear Phishing	No. of spam e-mail	Individual	C_{Ind}
Network Scanning	No. of packets No. of bytes No. of active flows	Technical Technical Technical	C_{Tech} C_{Tech} C_{Tech}
Malware	Process utilisation Memory utilisation	Technical Technical	C_{Tech} C_{Tech}

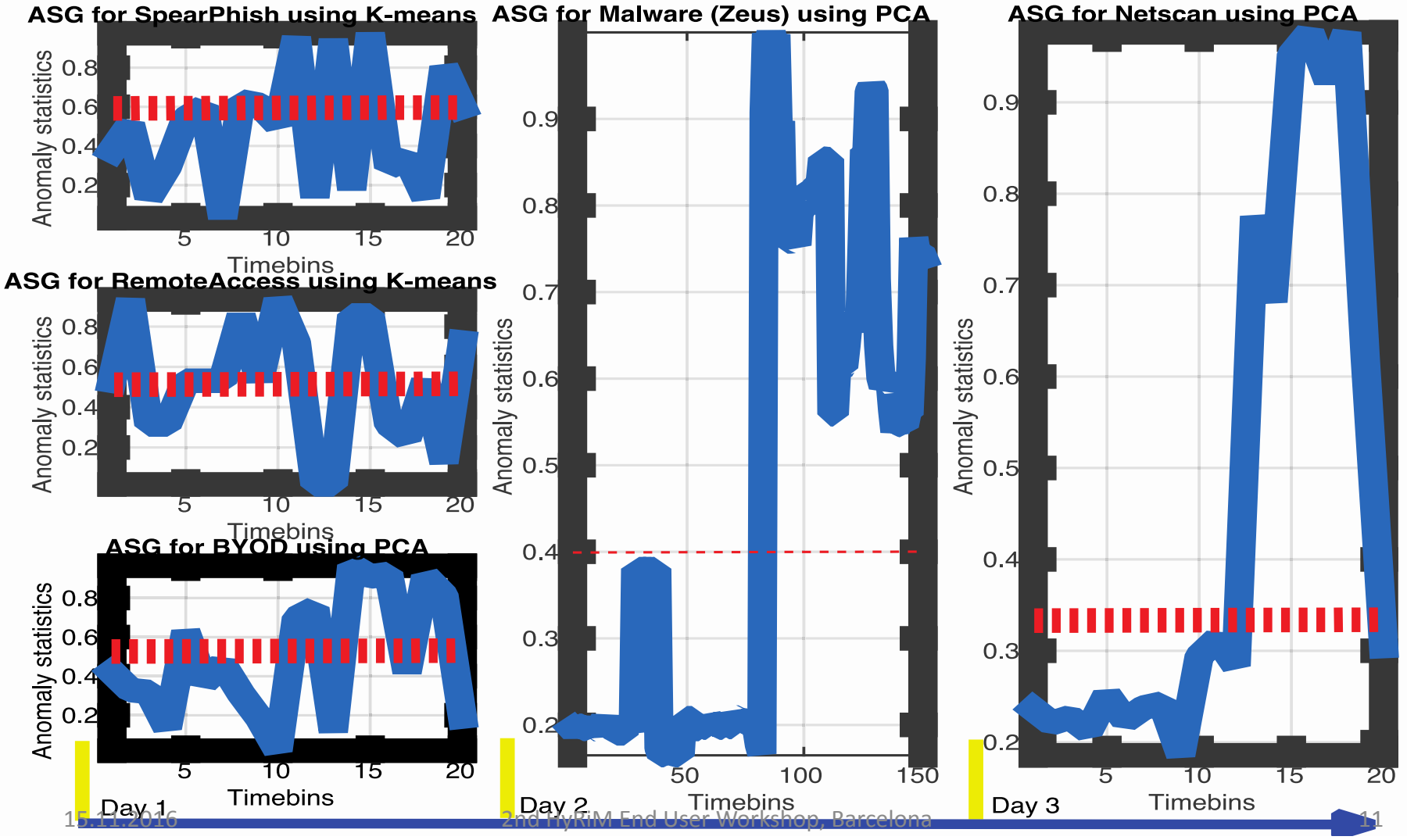
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Evaluation Testbed

- Two hosts with Kernel Virtual Supervisor
- Apache HTTP daemon
- Volatility introspection library
- 10-minutes runs
- Anomaly Detection Techniques
  - K-Means
  - Principal Component Analysis

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Evaluation



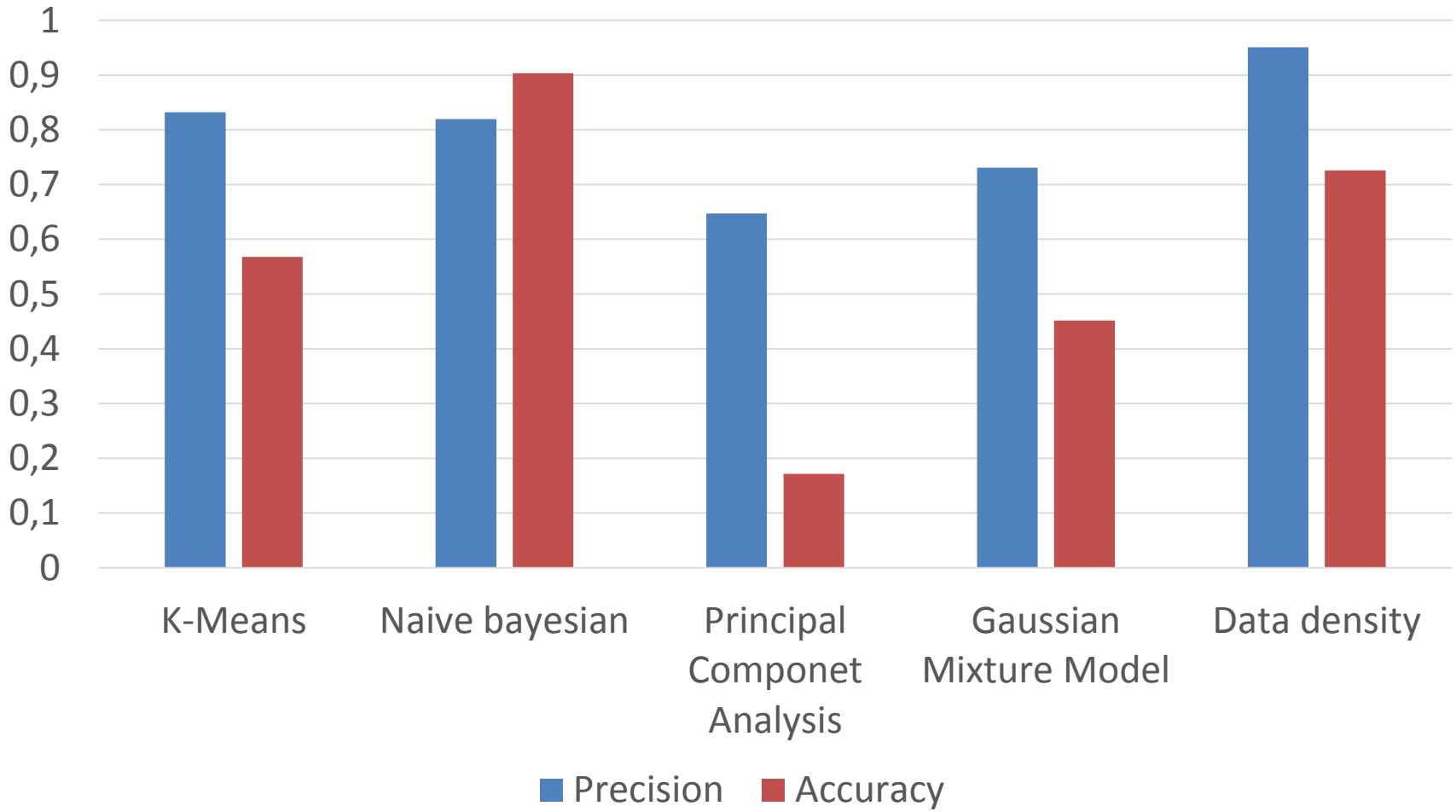
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

Evaluation of SCADA attacks

- Dataset: *'Morris, T., Thornton, Z., Turnipseed, I., Industrial Control System Simulation and Data Logging for Intrusion Detection System Research. 7th Annual Southeastern Cyber Security Summit. Huntsvile, AL. June 3 - 4, 2015.'*
- Gas pipeline log, captured in a laboratory environment, including:
  - Normal operation
  - Cyber-attacks
    - Response injection
    - Reconnaissance
    - Denial-of-Service
    - Command injection

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Comparison of AD techniques



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Conclusion and Future Steps

- Currently offering monitoring and detection services
  - Data Density algorithm
    - Unsupervised and memory less
- Identify threats using the OTI viewpoints
- Integrate our testbed/platforms
- Investigate the analysis and management planes

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Questions?