PHOENI2X - A European Cyber Resilience Framework With Artificial-Intelligence-Assisted Orchestration, Automation and Response Capabilities for Business Continuity and Recovery, Incident Response, and Information Exchange

George Daniil

University of Patras

14/12/2023

This project has received funding from the Horizon Europe Research and Innovation programme under Grant Agreement No101070586

Outline

- Introduction to the PHOENI2X framework
- Main innovation directions
- Use-cases and threat scenarios
- Summary and next steps

Outline

- Introduction to the PHOENI2X framework
- Main innovation directions
- Use-cases and threat scenarios
- Summary and next steps

PHOENI2X framework overview

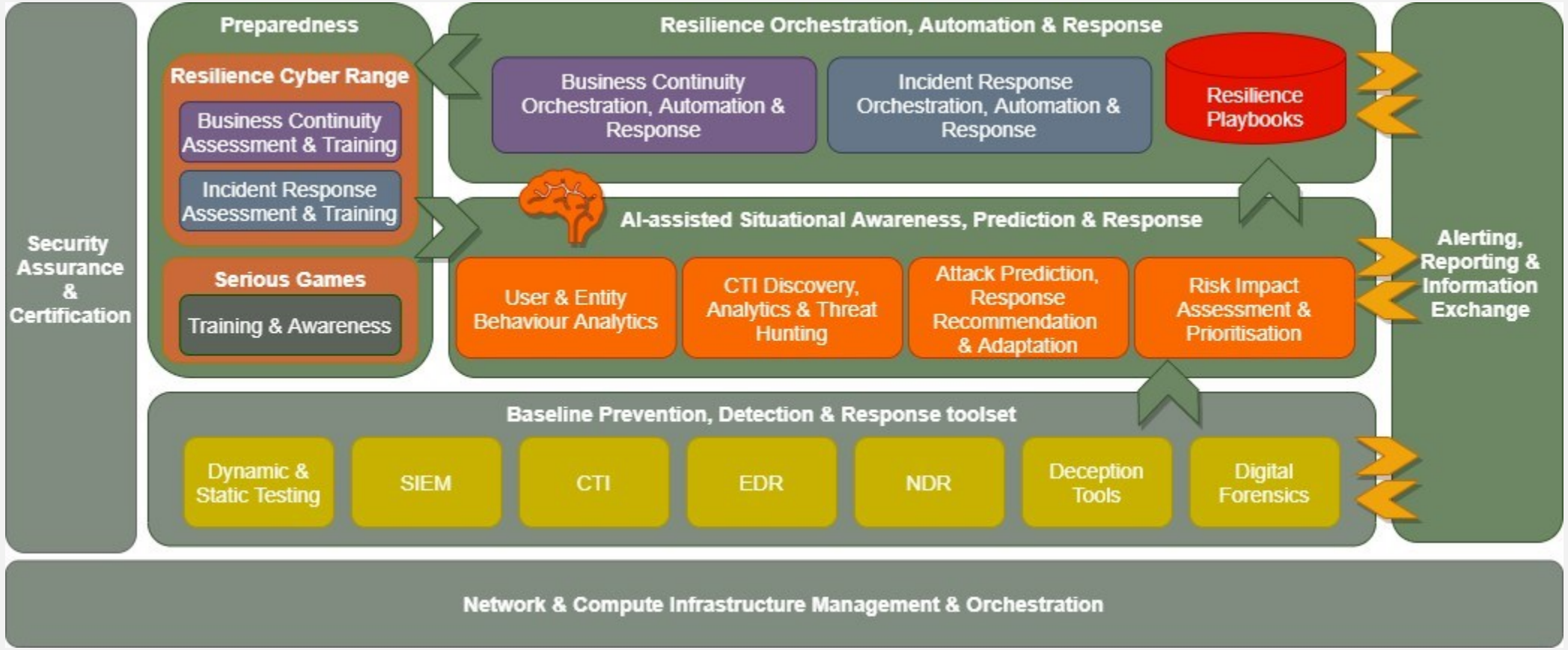
- PHOENI2X aims to design, develop, and deliver a Cyber Resilience Framework providing Artificial Intelligence (AI) - assisted orchestration, automation & response capabilities for business continuity and recovery, incident response, and information exchange
- Tailored to the needs of Operators of Essential Services (OES) and of the EU Member State (MS) National Authorities entrusted with cybersecurity.
- Aligned with the pertinent EU initiatives, such as the recommendations provided in the European Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ("Cyber Blueprint") & supporting the newly launched Cyber Crisis Liaison Organization Network (CyCLONe).

PHOENI2X will assist operators of critical sectors achieve cyber resilience & also support EU MS authorities in enhancing national cybersecurity capabilities, cross-border collaboration, and national supervision of their critical sectors, per the NIS Directive's requirements.

Key approach objectives

- Through PHOENI2X Cyber Resilience Centres (**PHOENI2X CRCs**), OES will gain:
  1) Enhanced Situational Awareness with AI-assisted Prediction, Prevention, Detection & Response capabilities, and business risk impact assessment-based prioritisation
  2) Proactive & reactive Resilience Automation, Orchestration, and Response (ROAR) mechanisms, providing Business Continuity, Recovery and Cyber & Physical Incident Response
  3) Increased Preparedness through relevant Serious Games and realistic Resilience Cyber Range (RCR) Assessment & Training
  4) Timely and actionable Information Exchange between OES, National Authorities and EU actors, leveraging interoperable and standardised alerting and reporting mechanisms and processes

PHOENI2X conceptual architecture



Baseline prevention, detection and response toolset

- Dynamic and static vulnerability testing
- Security Information and Event Management
- CTI management and sharing
- Endpoint Detection and Response
- Network Detection and Response
- Deception tools
- Forensics tools

Outline

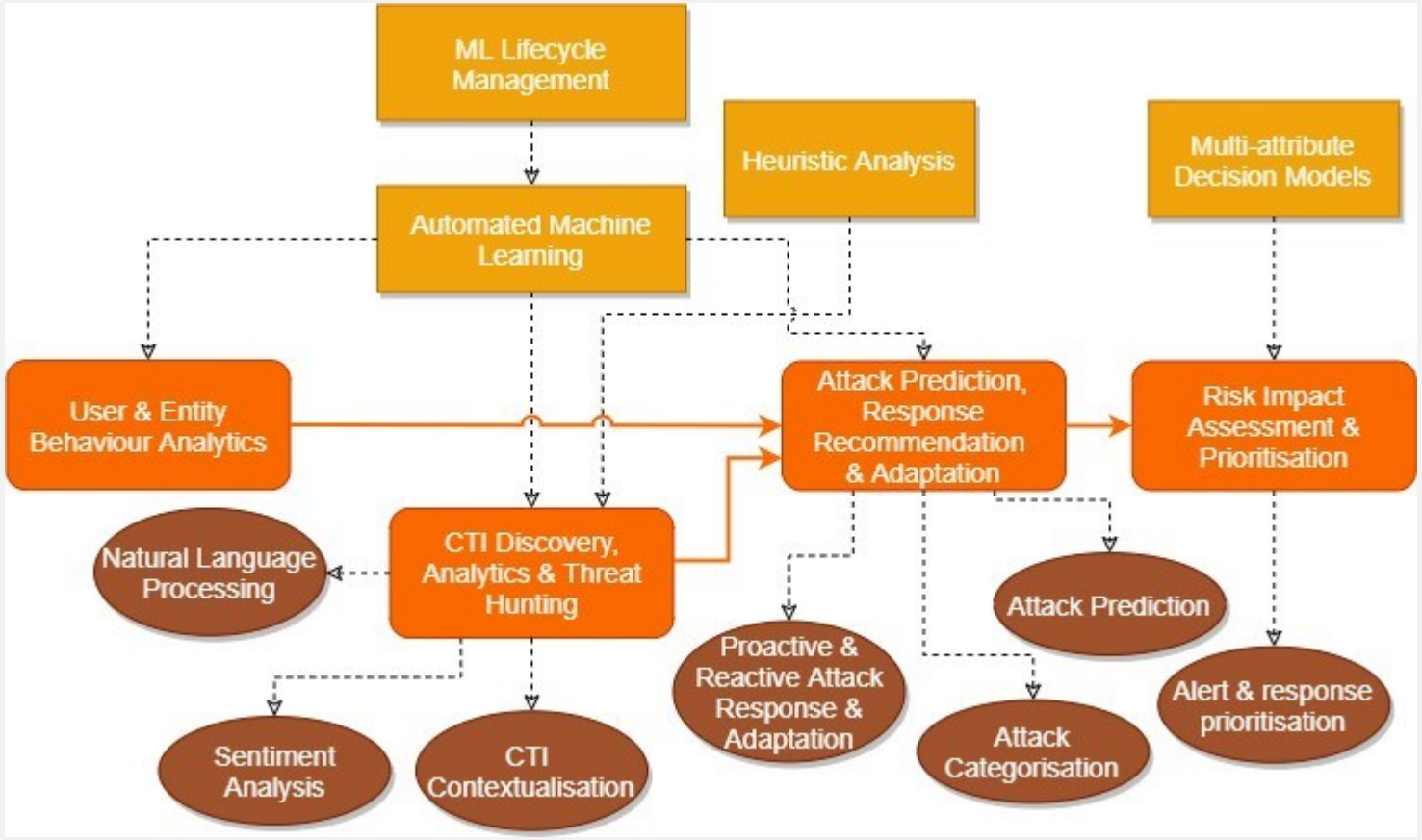
- Introduction to the PHOENI2X framework
- Main innovation directions
- Use-cases and threat scenarios
- Summary and next steps

Preparedness through Cyber Range & Serious Games

- Realistic scenario assessment and training capabilities through the integration of an Resilience Cyber Range (RCR) and Serious Games
  1) Assessment of defined Resilience Playbooks (e.g., to find gaps or inefficiencies, adapting them as needed)
  2) Hands-on training to OES staff in the business continuity, recovery and IR procedures encoded in the RPs
- Serious Games will support the RCR, focusing on the Training and Awareness of employees on different cyber attacks, threat elicitation, and improving organizational defenses that depend critically on human factors (e.g., social engineering and phishing attacks)

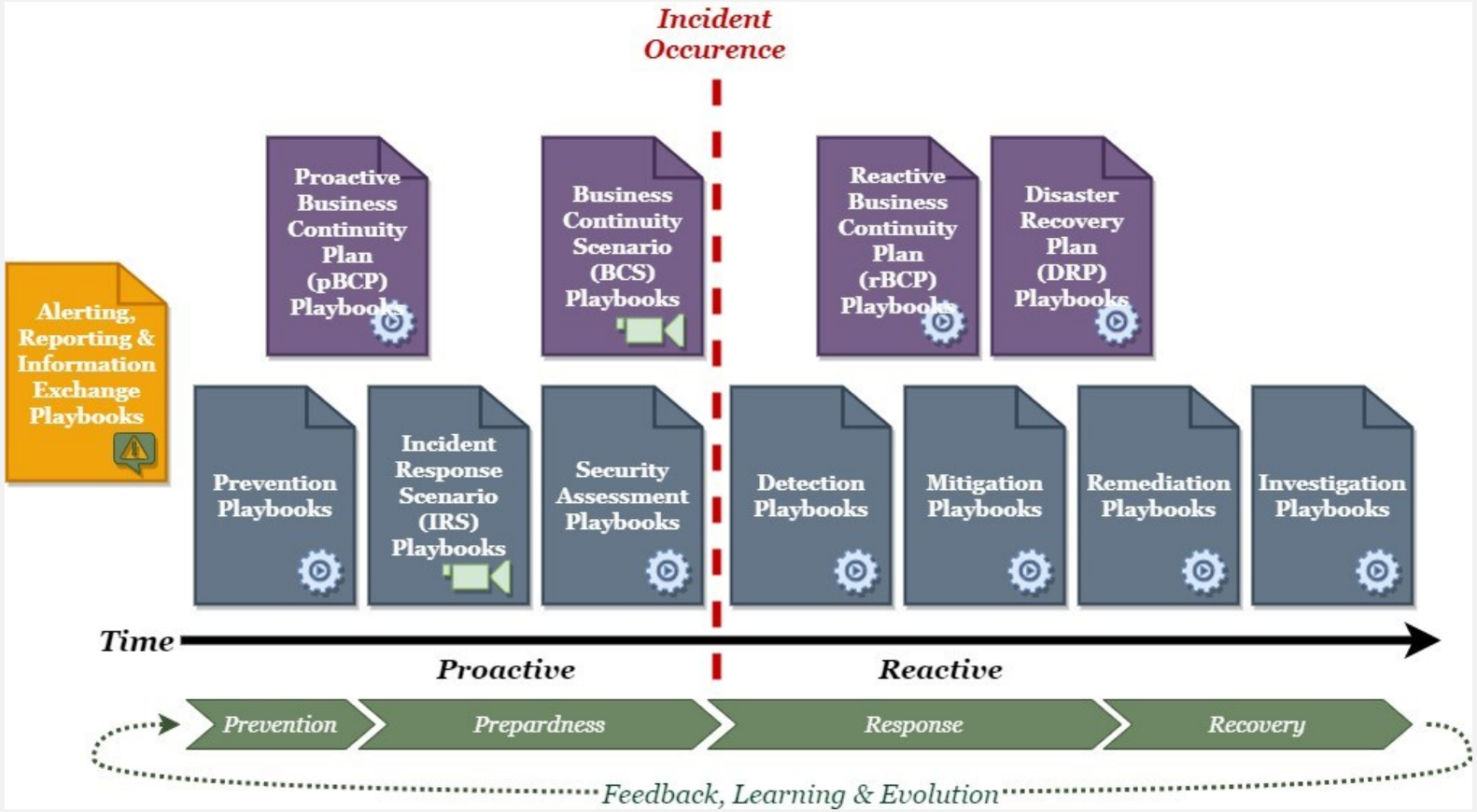
AI-assisted Situational Awareness, Prediction & Response

- **User & Entity Behaviour Analytics**, relying on an AutoML system to minimise overhead for data scientists and facilitate model selection.
- **CTI Discovery, Analytics & Threat Hunting**, leveraging AI (NLP, Sentiment Analysis, Heuristic Analytics) for the discovery, extraction, ingestion, correlation, and contextualization of CTI indicators.
- **Attack Prediction, Response Recommendation & Adaptation**, supporting attack categorization , attack prediction , and attack response and adaptation
- **Risk Impact Assessment & Prioritisation**, evaluating in near real-time the risk faced by an organisation qualitatively & quantitatively



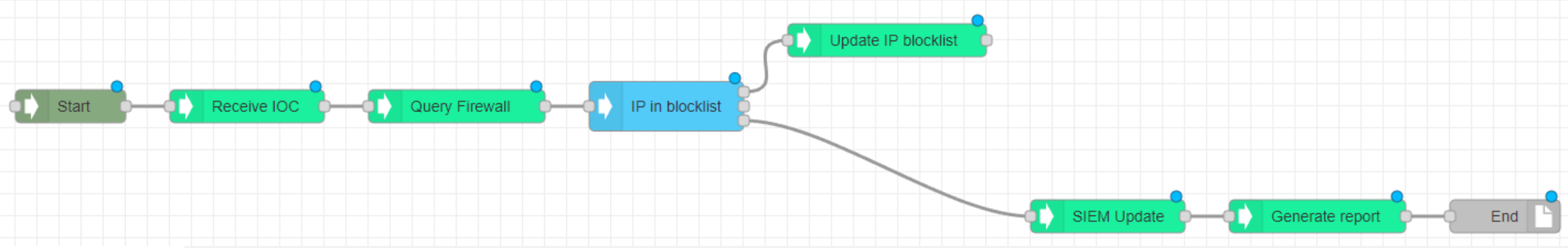
Automation through aspect-oriented playbooks

- **Adaptable and contextualizable** (e.g., by inputs from the AI-assisted Situational Awareness capabilities of PHOENI2X and post-incident analyses)
- **Customisable** to intrinsic requirements of every OES
- **Shareable** across organisation boundaries **at machine-speed**
- **Supporting what-if analyses**, with the specification of orchestrations involving components and capabilities that are not (yet) present in the organisation, and
- **Translatable** to support assessment and training in a realistic, simulated/emulated cyber range environment



Resilience Orchestration, Automation & Response (ROAR)

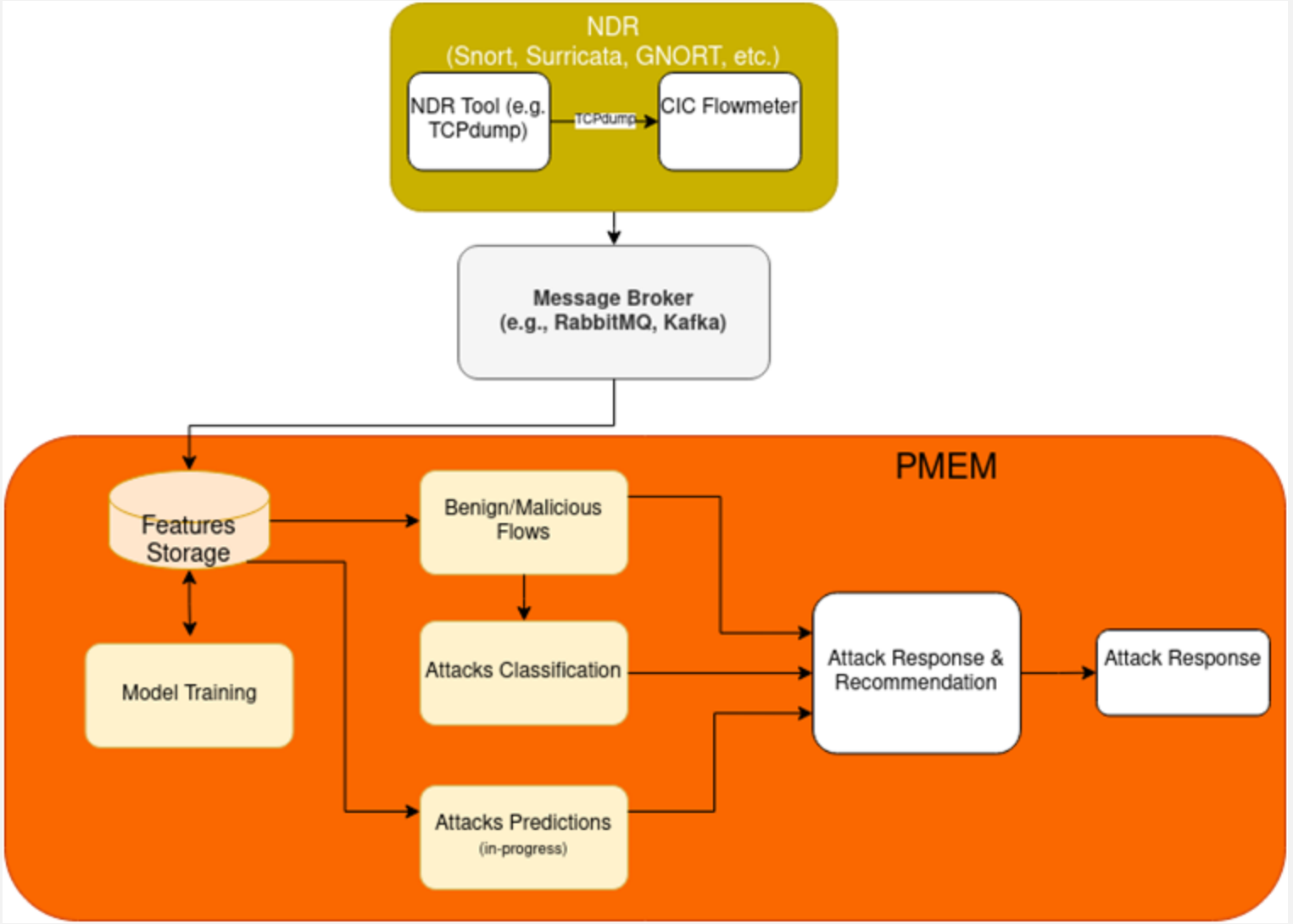
- Resilience Playbooks (RP): structured, machine-processable encoding of a sequence of actions comprising the organization's business continuity, recovery, and IR processes
- PHOENI2X adopts and extends the recently released OASIS Collaborative Automated Course of Action Operations (CACAO) specification



Predictive Maintenance (PMEM)

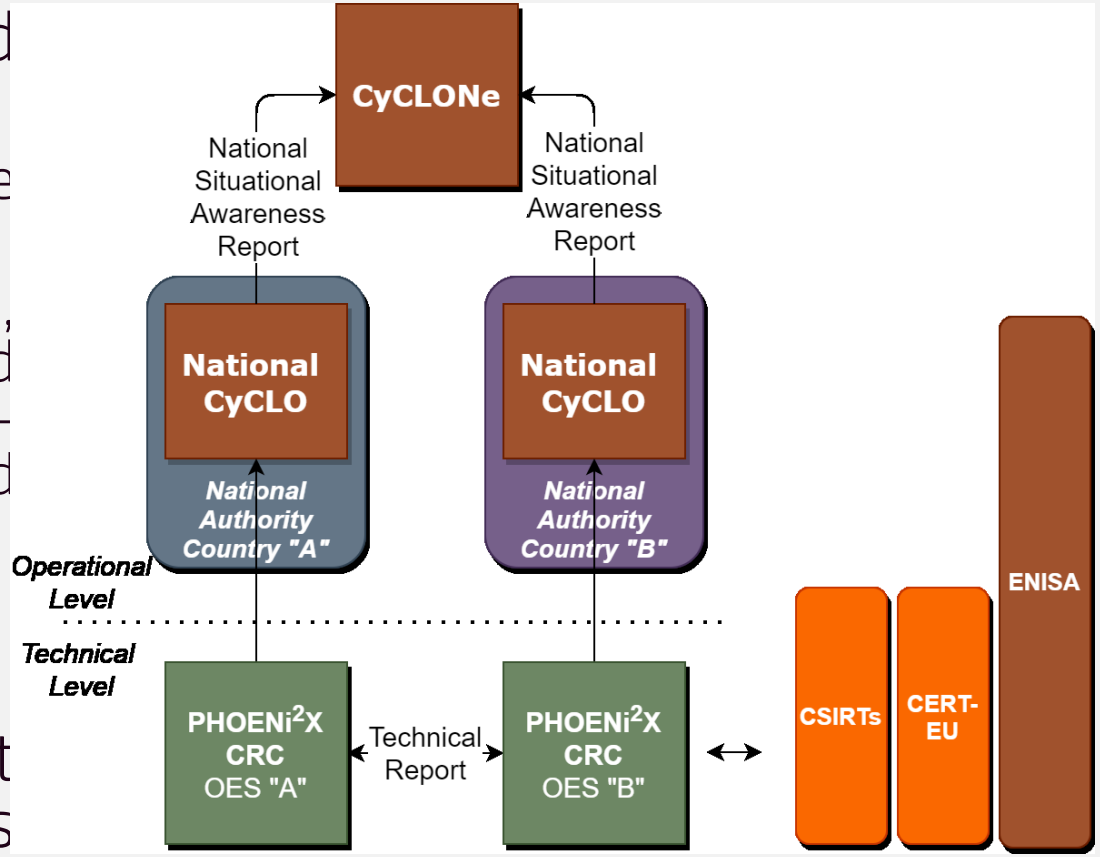
- Strong need for efficient predictive analytics-based approaches that utilize AI strategies to detect and predict known attacks along with ever-emerging zero-day exploits which can happen in the network

- PMEM uses supervised and unsupervised learning approaches to predict intrusions and propose specific actions as proactive actions to prevent the attack or as a response to the attack



Alerting, reporting and information exchange

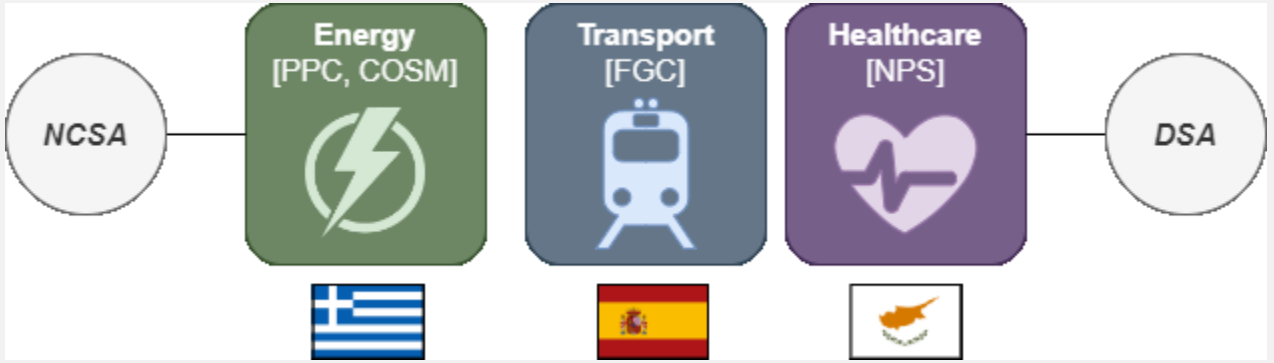
- Information exchange platform to address the need for standardized and coordinated cyber-security notifications as:
  1) Technical-level indicators from the Baseline Prevention, Detection and Response toolset
  2) AI-generated insights, early-warning alerts, contextualized information - CTI, models, and other shareable information from the AI-assisted Situational Awareness, Prediction and Response enablers
  3) RPs from the ROAR subsystem
  4) Training programs from the RCR
- Goal lies in linking all the EU-level relevant parties at the strategic and political level, as well as cyber-security IR actors (CSIRTs network, ENISA, NIS CG, CyCLONe)



Outline

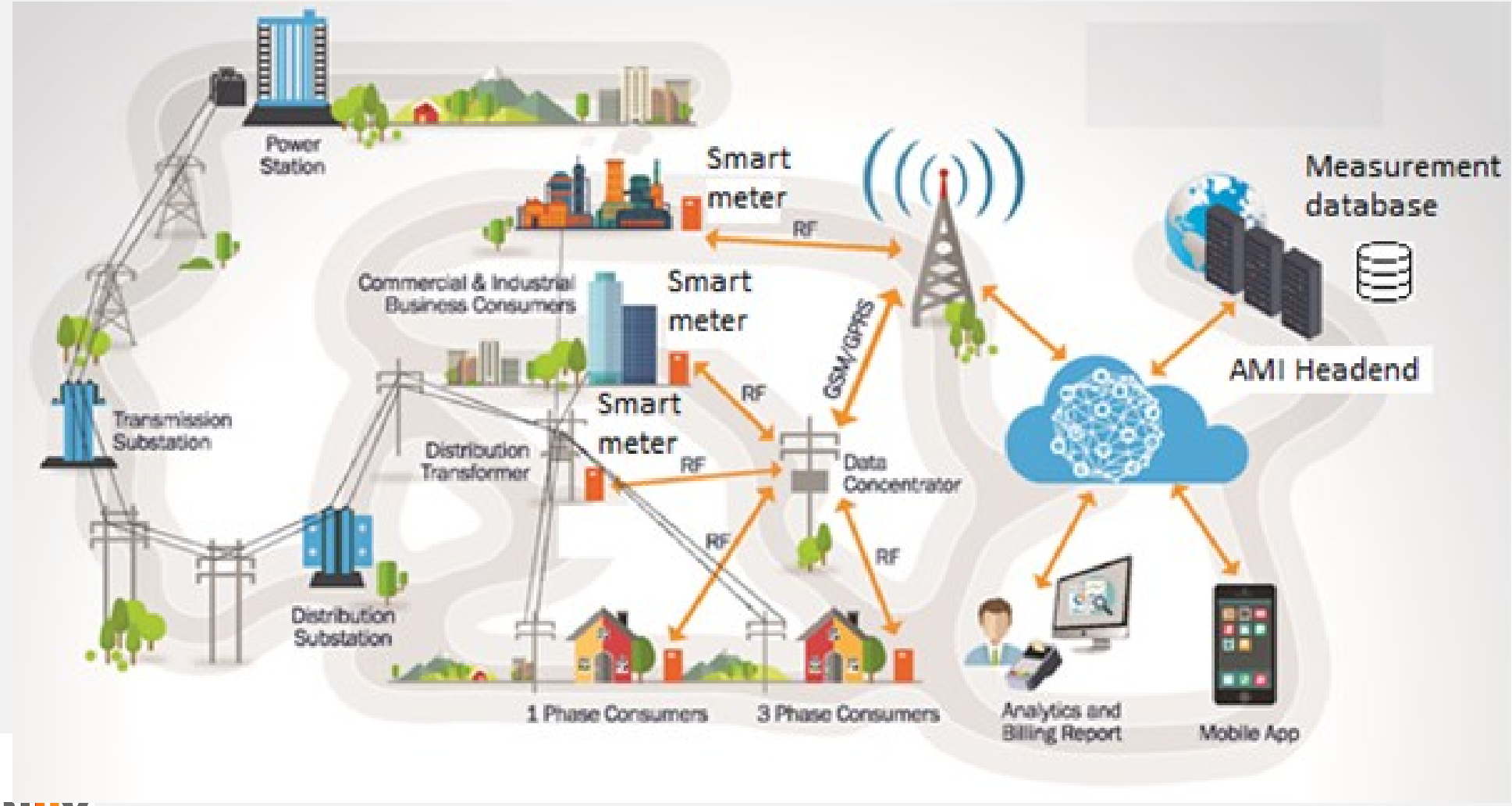
- Introduction to the PHOENI2X framework
- Main innovation directions
- Use-cases and threat scenarios
- Summary and next steps

Use-case overview

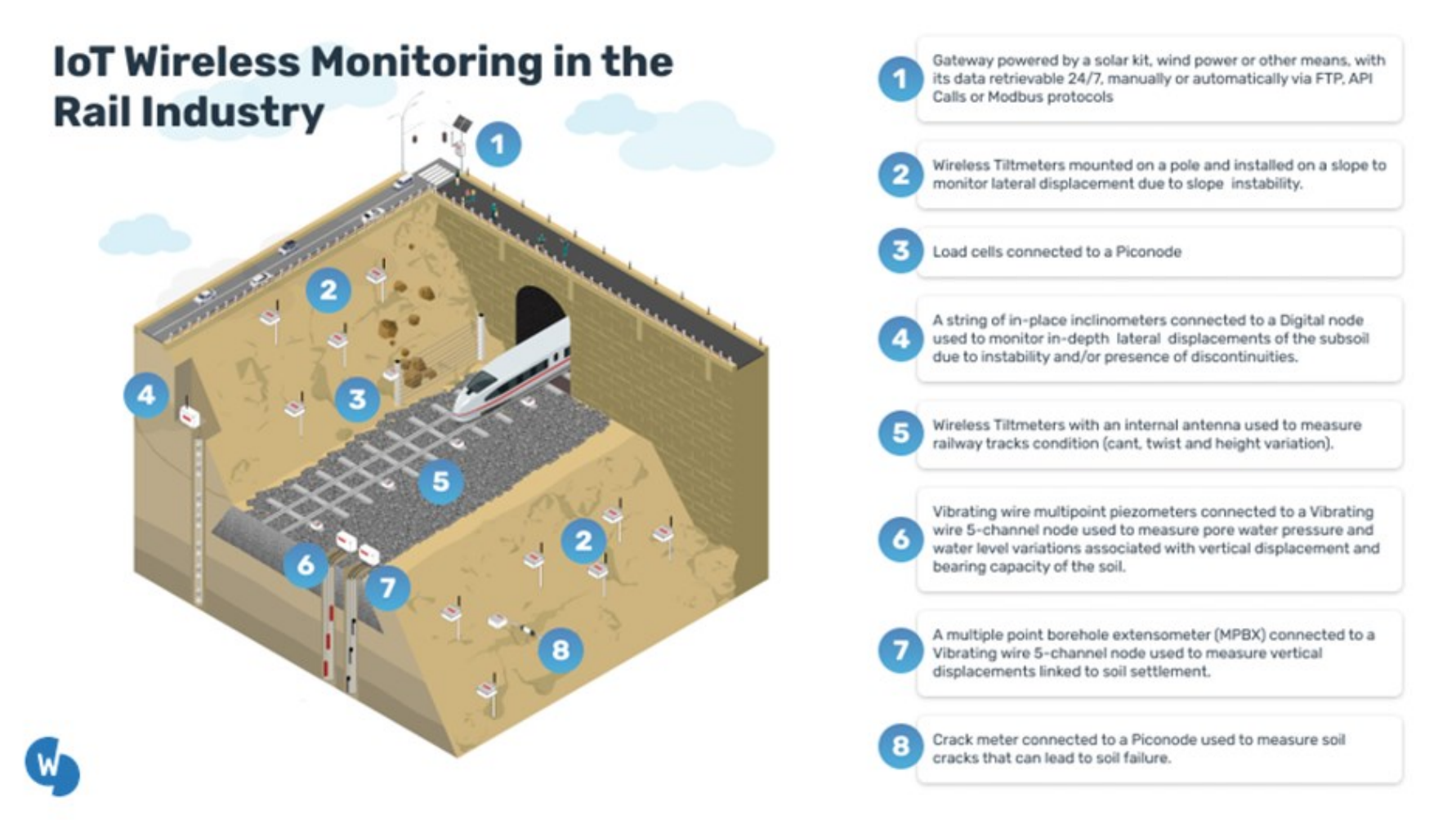


1. **Energy use case**, based in **Greece**, directly involving an OES (Public Power Corporation) as well a supporting telecom provider and the National Authority (**NCSA**) overseeing the OES
2. **Transport use case**, based in **Spain**, directly involving an OES
3. **Healthcare use case**, based in **Cyprus**, involving an essential solution and infrastructure provider of an OES (the General Healthcare System of Cyprus), to highlight the importance of supply chain aspects, and the National Authority (**DSA**) overseeing the OES

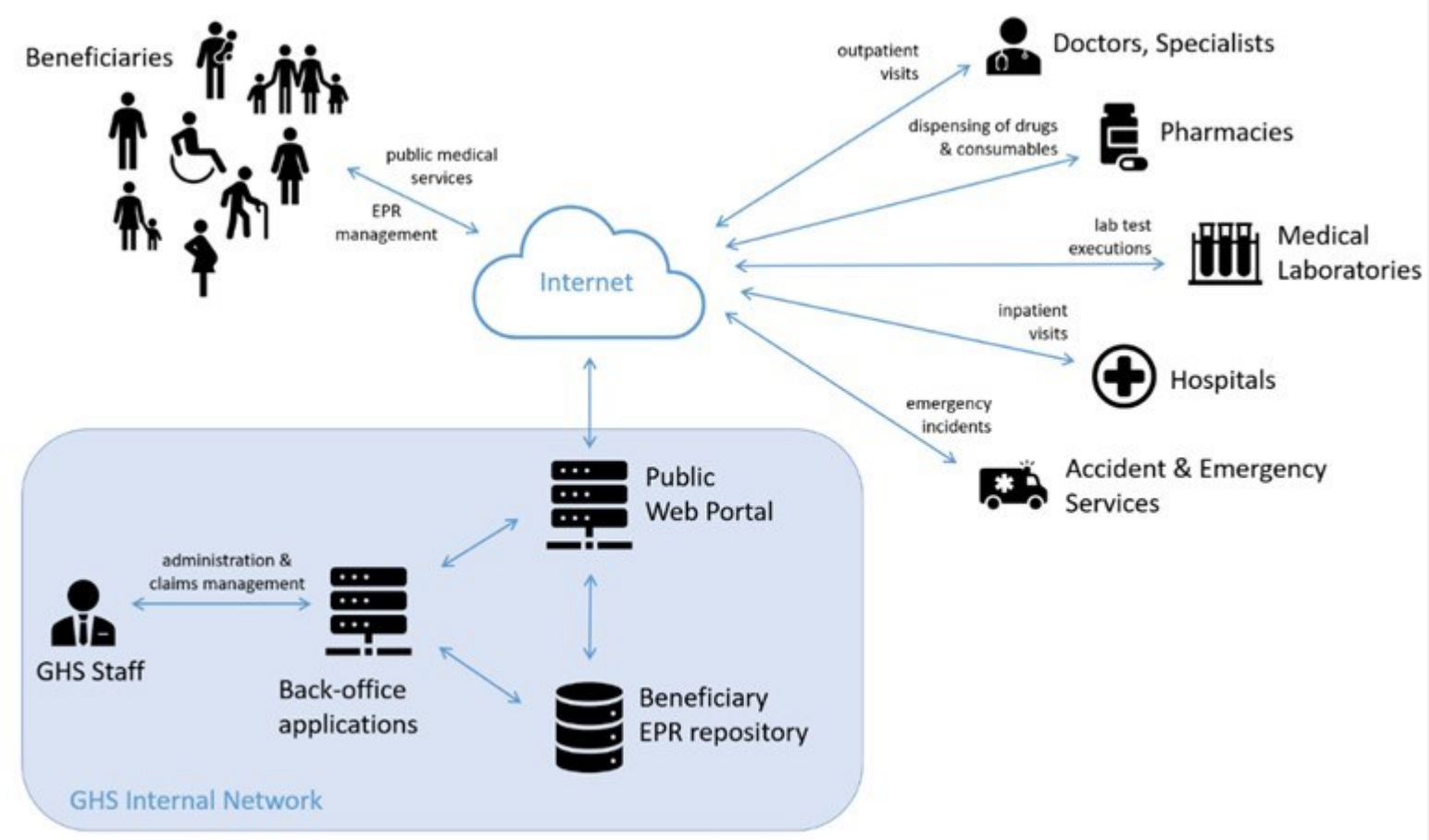
Use-case 1: Cascading effects of cyber attacks against advanced metering infrastructure



Use-case 2: Cyber and physical attacks and risk management service for the railway management system



Use-case 3: cyber attacks aiming to cripple the public healthcare system



Outline

- Introduction to the PHOENI2X framework
- Main innovation directions
- Use-cases and threat scenarios
- Summary and next steps

Summary and ongoing work

- AI-enhanced Cyber Resilience Framework, providing orchestration, automation and response capabilities for business continuity and recovery, IR, and information exchange
- Individual components comprising PHOENI2X will be developed and integrated
- Deployment and testing of tools against both known and zero-day threats and attacks in the Energy, Transport, Health sectors
  - Validation, reporting and information exchange from National cyber-security Authorities
- Holistic assessment of PHOENI2X and its vision, collecting concrete evidence of its applicability, along with valuable feedback and pointers for its further refinement

Consortium

Public
Power
Corporation

SOCIAL
ENGINEERING
ACADEMY

Eunomia Ltd.
Consulting Services

UiO : University of Oslo

Thank you for your attention!!
Questions?

Phoeni2x.eu

gdaniil@ece.upatras.gr

This project has received funding from the Horizon Europe Research and Innovation programme under Grant Agreement No101070586