

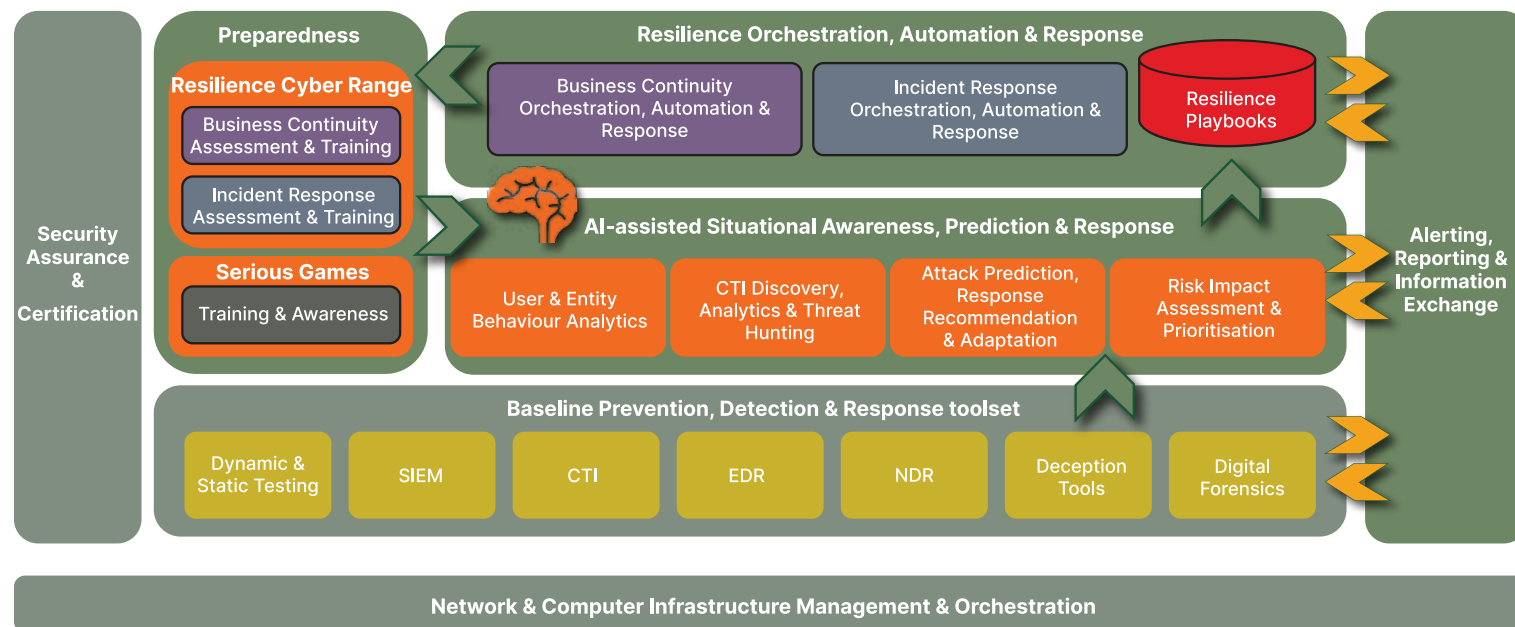
Towards Cyber Resilient European Infrastructures



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

*A European Cyber Resilience Framework with Artificial Intelligence (AI)
– assisted orchestration & automation for business continuity,
incident response & information exchange*

PHOENIX2X aims at delivering a Cyber Resilience Framework providing Artificial Intelligence (AI) – assisted orchestration, automation and 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 National Authorities entrusted with cybersecurity.



Use Cases

ENERGY

The Energy use case will strengthen the Advanced Metering Infrastructure (AMI) security and operational resilience of the Energy Operator during disruptions, such as cyber-attacks, while the Telecom Operator provides a fallback communication channel between the customer and the AMI Headend. The PHOENIX2X platform also facilitates timely reporting to the National Competent Authority, ensuring regulatory compliance and effective incident management.

TRANSPORT

The Transport use case will deploy the next generation services for a digital railway infrastructure improving the proactive strategy to predict cyber-attacks, identifying and isolating security and safety threats of train operations by subdividing the system in 3 layers: data collection, data processing and data analytics.

HEALTHCARE

The Healthcare use case will build security solutions to ensure business continuity focusing on supply chain attacks targeting the delivery pipeline to preserve the General Healthcare System of Cyprus from malicious code deployment in the production servers, which could severely impact portal functionality, and even disrupt the healthcare operations of the entire country.