PHOENIIX

# Energy

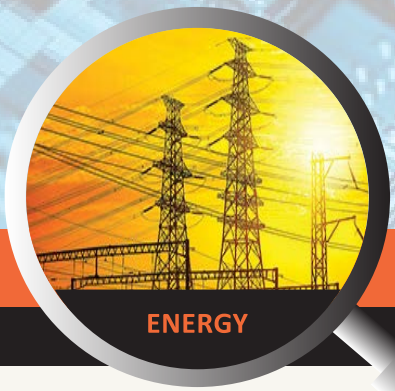
## Pilot Description

An Advanced Metering Infrastructure (AMI) testbed is deployed, comprising DLMS/COSEM smart meters, a head end server and a field PHOENI2X Secure Gateway that bridges OT and IT networks.

## Incident Scenarios

| Phase | Highlighted events | Key PHOENI2X components in action |
|---|---|---|
| **Prevention & Preparedness** | Continuous monitoring of meter traffic and host logs; periodic vulnerability and CTI assessments; Employees continuous training. | **NDR and PMEM** monitors network traffic for anomalies, **EDR** captures host artefacts, **SIEM** correlates events, **CTI/TII** inject fresh threat indicators. **CERCA** merges all evidence to compute business risk scores, while **ResilienceCR** (Serious Games + Resilience Cyber Range) provide tailored training and cybersecurity awareness. |
| **Scenario 1**<br>**Large scale DDoS** | A volumetric flood targets the AMI head end, attempting to exhaust bandwidth and processing. | **PMEM** detect traffic spikes, push an alert to **CERCA**, which ranks response playbooks. **ROAR** executes the top priority playbook, throttling malicious flows and isolating rogue IPs; **SMIR** created the incident case report. Additionally attacks against a **Smart Meter Honeypot** deployed at the pilot network captures the malice's activities and sends them to **FVT** for further analysis. |
| **Scenario 2**<br>**Physical link sabotage** | The primary communication link to a remote meter is severed. Back-up communication channel is enabled automatically without human interention. | The **Secure Gateway** senses the outage, switches to a back up channel and notifies **ROAR**. ROAR's business continuity playbook documents actions in **SMIR** and informs the operator via **FVT**, preserving data collection and incident tracking without manual intervention. |
| **Post Incident** | Investigation, reporting and model update. | **FVT** allows the operator to perform root cause analysis of the incident; **TII** enriches the report with a CTI score and additional information; **SMIR** produces an NIS2 aligned incident report that is automatically sent to the National CSIRT. Findings feed back into **CERCA** to refine future risk assessments. |

PHOENIIX




## PHOENI2X Solution

- **Enhanced Situational Awareness:**
  *NDR, PMEM, EDR, SIEM and CTI/TII* stream unified telemetry into **CERCA,** whose AI models predict threats, detect anomalies and prioritise responses by business impact.
- **Resilience Automation, Orchestration & Response (ROAR):**
  Orchestrated playbooks span cyber (DDoS mitigation, malicious host isolation) and physical (link fail over) events, ensuring seamless **Business Continuity, Recovery and Incident Response** while every action is case managed in **SMIR**.
- **Operator Preparedness:**
  The **Resilience Cyber Range (RCR)** together with **Serious Game modules**, deliver immersive exercises tailored to the Energy sector and personalised feedback, continually increasing the security awareness and readiness of the employees.
- **Timely, Standards Based Information Exchange:**
  **SMIR** auto generates structured reports (STIX/TAXII, ISAC formats) that flow between the Operator of Essential Services, National Authorities and EU actors.

As a result the pilot through PHOENI2X is able to sustain resiliency of its metering services - predicting attacks, automating defense, training people, and reporting outcomes - in one integrated, AI assisted framework.

## Consortium

University of Patras
Sphynx
Universitat Politècnica de Catalunya BarcelonaTech
OTE Group of Companies
FGC Ferrocarrils de la Generalitat de Catalunya
AEH
World Sensing
AEGIS IT Research
Social Engineering Academy
Eunomia Ltd. Consulting Services
Atos
APIROPLUS SOLUTIONS
Nodalpoint
UiO : University of Oslo
National Cyber Security Authority GR
National CSIRT-CY

phoeni2x.eu/ @Phoeni2xProject @Phoeni2xEUProject @Phoeni2x