For more details contact:

Ghasan Bhatti
Project Coordinator
Capgemini Technology Services, France
ghasan.bhatti@capgemini.com

PHOENIX Admin Team
phoenix-info.fr@capgemini.com

Join Us

@H2020Phoenix

company/phoenix-h2020/

https://phoenix-h2020.eu/

PHOENIX

PHOENIX

EU H2020

Electrical Power System's Shield against complex incidents and extensive cyber and privacy attacks

The project has received funding from the European Union's Horizon2020 research and Innovation programme under grant agreement N°832989. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

PHOENIX Objectives

- **Strengthen EPES cybersecurity preparedness** by employing

a) "security by design" via novel protective concepts for resilience, self-healing, and accountability,

b) "security by innovation" via adapting, upgrading, integrating, and validating a number of TRL5 developments to TRL7-8.

- **Coordinate EPES cyber incident discovery, response and recovery**, contributing to the implementation of the NIS Directive by developing and validating at national and pan-European level, a novel fully decentralized near real-time synchronized information awareness exchange platform, among authorized utilities, CSIRTs, ISACs, CERTs, NRAs and the strategic NIS cooperation group.
- **Accelerate research and innovation in EPES cybersecurity** by a novel prevent, detect and mitigate DevSecOps mechanism, secure and privacy preserving federated Machine Learning (ML) algorithms and definition of certification methodologies and procedures.

PHOENIX makes society more secure and trustable

Securing the EPES infrastructures and enabling reliable access to EPES and personal data is a fundamental good for society. PHOENIX will make society more secure by:

- **Protecting existing and designing a new generation** of less vulnerable, more resilient and self-healing European EPES able to survive large scale, combined, cyber-human security and privacy incidents and attacks, and guarantee the continuity of operations.
- Economic impacts associated with **EPES and cascading effects will be reduced,** whereas the proposal of open APIs will ensure that the security holes hunting will be limited to a smaller number of use cases, rendering it more focused, thus effective.
- Closing **the digital gap.** PHOENIX intends to support social cohesion by enabling citizens and those currently excluded by the "digital divide" and "social exclusion" and to participate in **high quality digital services**.

PHOENIX as a security and privacy platform

PHOENIX aims to make a **significant impact by providing a cybersecurity solution** that will be able to **cover the existing market gap, providing not only a beyond the state-of-the-art IDS system**, but a **customizable platform, which can combine security and privacy SLAs** with reasonable cost.

PHOENIX is maybe the only effort **solely focused on EPES** taking into account Energy stakeholders' knowledge while adopting a **fully adaptive DevSecOps approach**. Moreover, it is a **combined security and privacy toolbox**, which **inherently supports the NIS Directive implementation** via a secure and traceable Incidents Information Exchange Platform (I2SP).

I2SP: the cornerstone of PHOENIX Platform

The Incidents' Information Sharing Platform (I2SP), via its embedded secure and trusted CTI information sharing, state-of-the-art ML analytics, and optimal countermeasure and mitigation provisioning tools offer **major cybersecurity enhancements to the EPES inherent cybersecurity shield.** The I2SP provides to the interconnected parties:

- High-quality CTI data generation structured in standardized format STIX v2.1
- Regional, national and Pan-European coordinated and cascading effects identification
- Early alarm generation and countermeasure coordination
- Visualization of cybersecurity attacks and threats at Pan-European level

PHOENIX I2SP by design is aligned with the EU cybersecurity guidelines pertaining to the **Energy sector**. At the same time, **the I2SP role and accurate placement is proven** and further enhanced through vigorous monitoring of the advancements in EU cybersecurity spectrum that adhere to the relevant directives and policies (NIS, EU cybersecurity strategy, Network Code). Evidently, the **I2SP approach is "validated**" by **the Network Code** that is currently finalized by the participating **cybersecurity bodies**, including **ACER, ENTSO.E, E.DSO and ENISA.**

PHOENIX in pursuit of zero risk

The cybersecurity plans can never guarantee that the risk is set to "absolute zero". The race of protection vs attack is in the best case a "red queen`s race" that will go on and all we can do is to **increase detection of the systems and eliminate**, or decrease at least, the **human factor** in this process.
The integration of PHOENIX **highly contributes to increased protection against cybersecurity attacks** by **learning, adapting, and automating threat detection and mitigation**, as well as **threat information sharing,** supporting EPES in joining forces against malicious actors in their critical infrastructure.
At Phoenix, we aim to achieve it by incorporating **threat management at all levels of IT and OT** processes as well as imposing cybersecurity standards in external factors.

PHOENIX at ENLIT Europe 2021

PHOENIX project was presented at **Enlit Europe** from 30 Nov to 2 Dec 2021 in Milan, Italy. Enlit Europe gives a platform to numerous EU funded projects contributing to the **digitalisation of energy** which is in line with the purpose of the PHOENIX project.

PHOENIX results and platform capabilities were communicated to the event participants. Our consortia partners colleagues **(RWTH, DNV, CRE)** also participated as **Speakers and Panelists** in **three sessions** at the event and talked about the PHOENIX project.