

CyberSEAS

Cyber Securing Energy dAta Services

Update on
status and
main
achivements



Paolo Roccetti
Head of cybersecurity research unit
Engineering Ingegneria Informatica

Consortium and duration

- ▶ 26 organisations
 - ▶ 6 Energy Operators
 - ▶ 2 Smart Cities
 - ▶ 3 testing and certification labs
 - ▶ 14 Technology Providers
 - ▶ 1 Legal/regulatory support

- ▶ 3 years
 - ▶ started on 01/10/2021
 - ▶ Ending 30/09/2023

- ▶ ~10M€ budget
 - ▶ ~8M€ funding

- ▶ 10 involved Countries
 - ▶ Belgium, Croatia, Estonia, Finland, Germany, Greece, Italy, Romania, Slovenia, Spain,



Comune di Benetutti

Comune di Berchidda

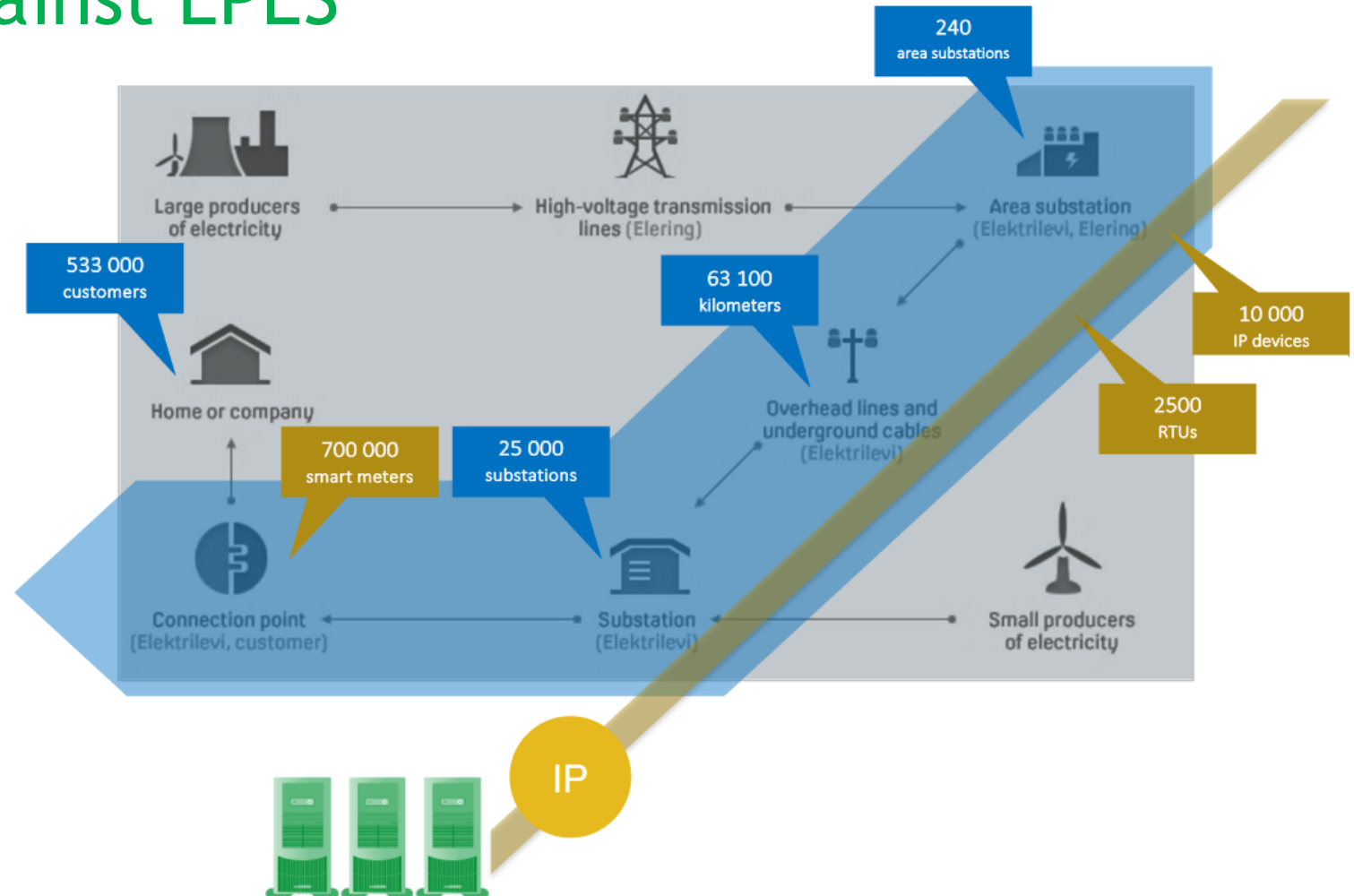


This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 101020560

CyberSEAS Strategic Objectives

S01: Countering the cyber risks related to the highest impact attacks against EPES

- ▶ disruption of the operational & business continuity
- ▶ substantial damage to infrastructures
- ▶ safety consequences (security induced safety cases)



S02: Protecting consumers against personal data breaches and cyber attacks

- ▶ protects consumer's personal data from consequences of cyber attacks
- ▶ protect the energy supply chain from attacks that exploit prosumers


ALPHV | Blog | Collections

GSE - Gestore Servizi Energetici
8/27/2022, 9:56:43 PM
site: <https://gse.it>
Downloaded **700GB** of data from the company's network, they include:

- Confidential data
- Accounting
- Contracts
- Reports
- Personal data
- Projects
- And many other internal documentation of the company

**In case of ignoring, we will publish this data!
For GSE companies: contact us by chat.**

Example:

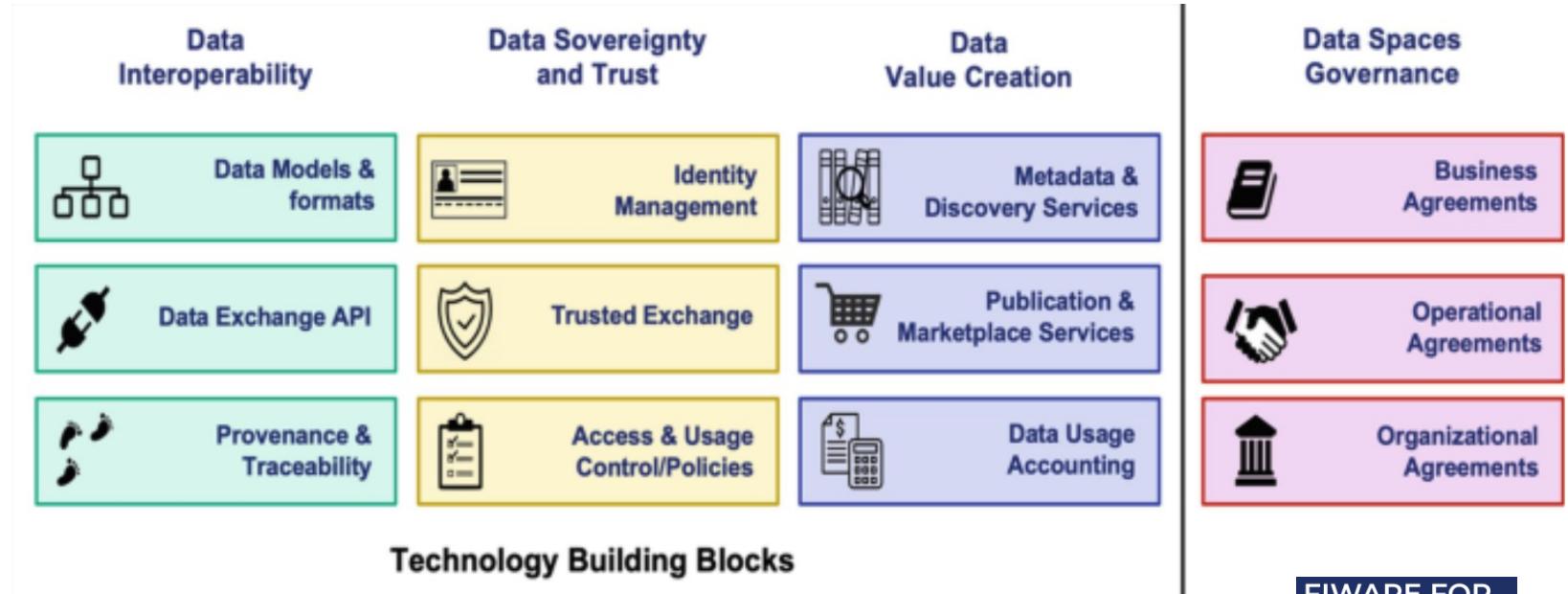


The screenshot shows the GSE logo (Gestore Servizi Energetici) and the text: "Amministratore Unico" and "PROT. N. GSE/SS/P2022/002 DEL 14 GENNAIO 2022".



S03: Increasing security of the Energy Common Data Space

- ▶ enhancing data space governance
- ▶ balancing the sensitivity of data vs. the need for real-time detection



FIWARE FOR
DATA SPACES



Main Achievements

Technical & Methodological Achievements

Real Use Cases



Architecture and Toolset



Validation

- ▶ Collaborative assessment of cyber vulnerability and risks in the energy supply chain

EU-RES

- ▶ First release of the CyberSEAS architecture and toolset

EU-RES

- ▶ Integration and validation plan & start of in-lab validation

EU-RES

- ▶ First version of methodological measures for securing Energy Data Space and operators



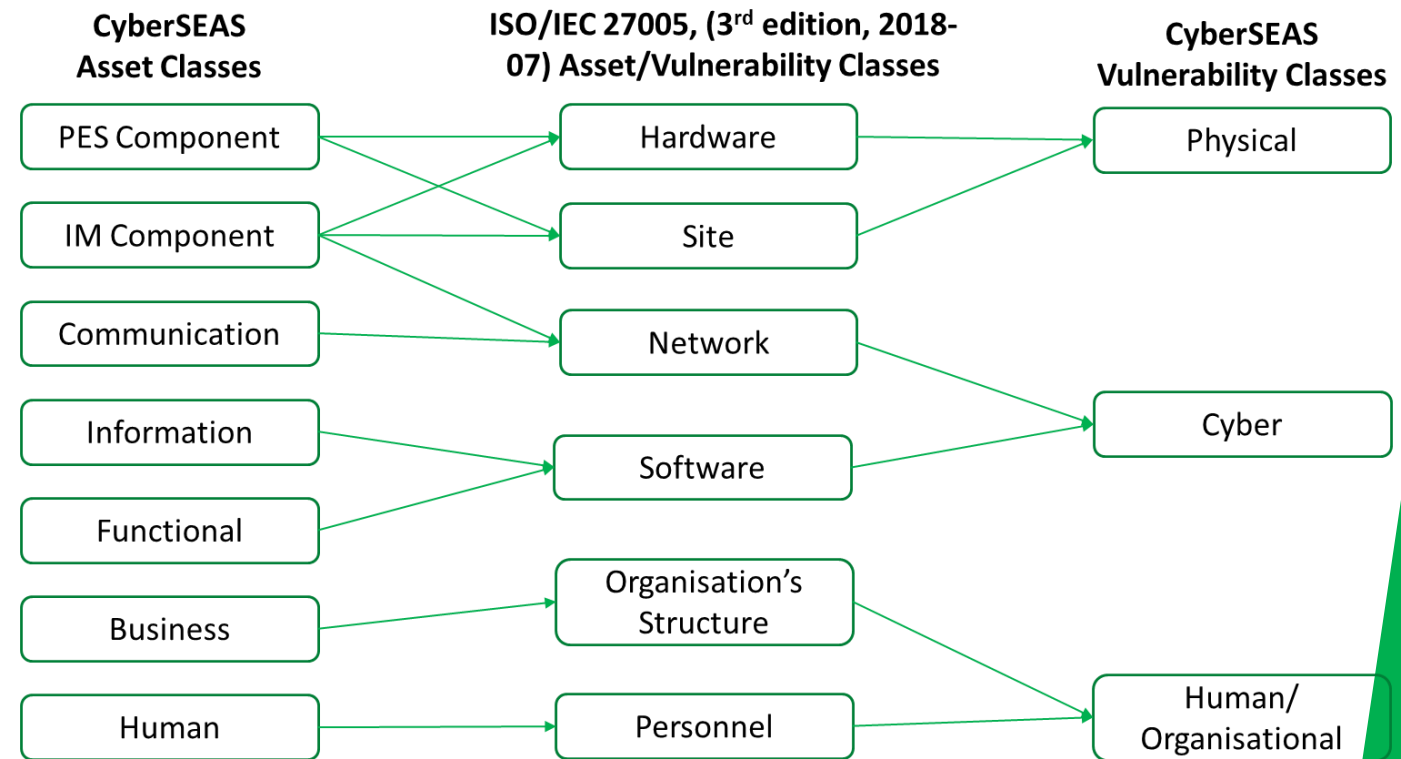
Vulnerability Analysis for the energy supply chain

- ▶ Asset identification and classification wrt SGAM architecture

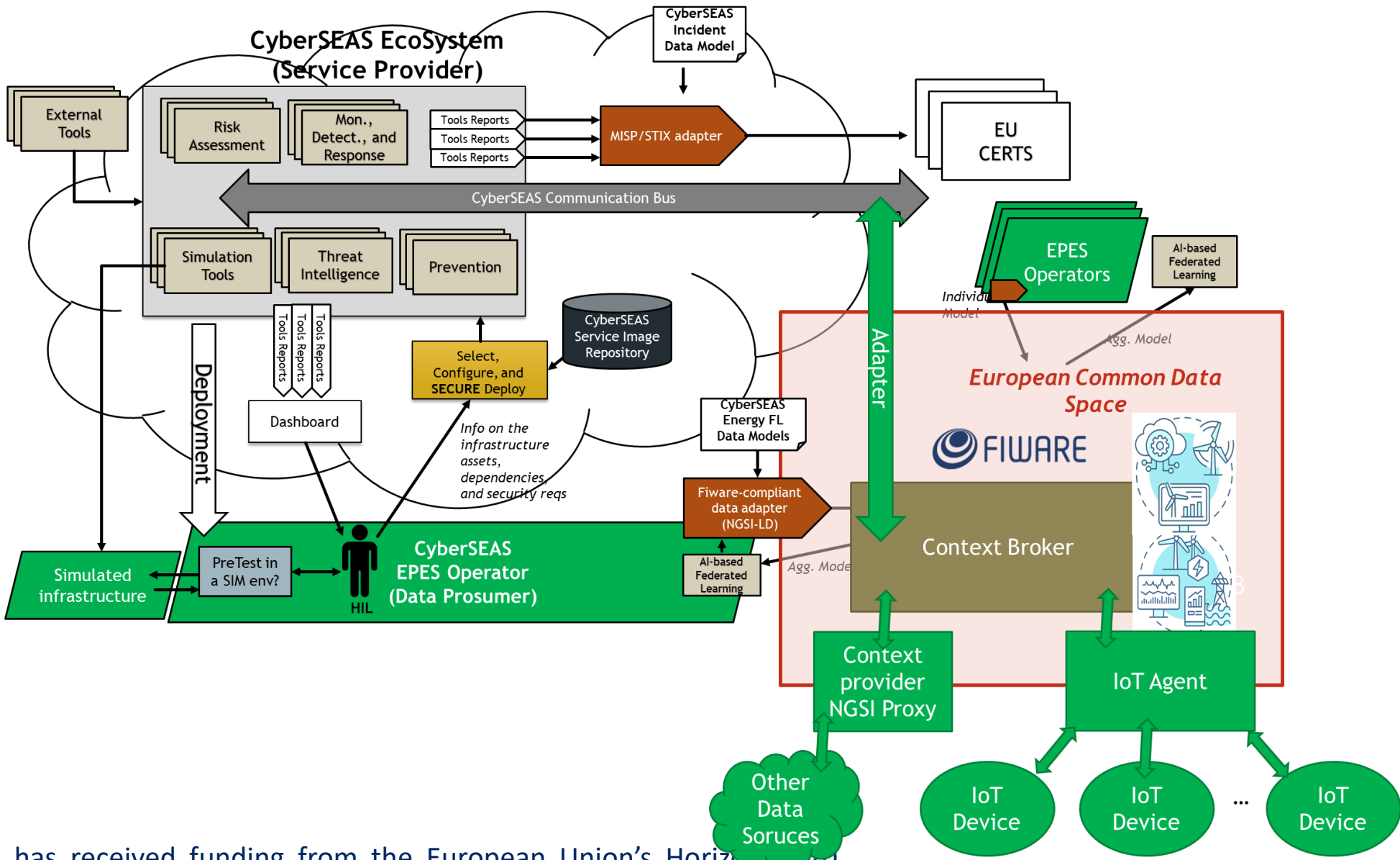
- ▶ Vulnerability elicitation

- ▶ Static: NESCOR, ISO/IEC:27005, NIST without NESCOR, and pilot contributions
- ▶ Dynamic: pentesting performed by technical providers against infrastructures
- ▶ **Over 220 vulnerabilities** collected and analysed

- ▶ Vulnerability assessment and ranking done jointly between infrastructure owner and technical provider

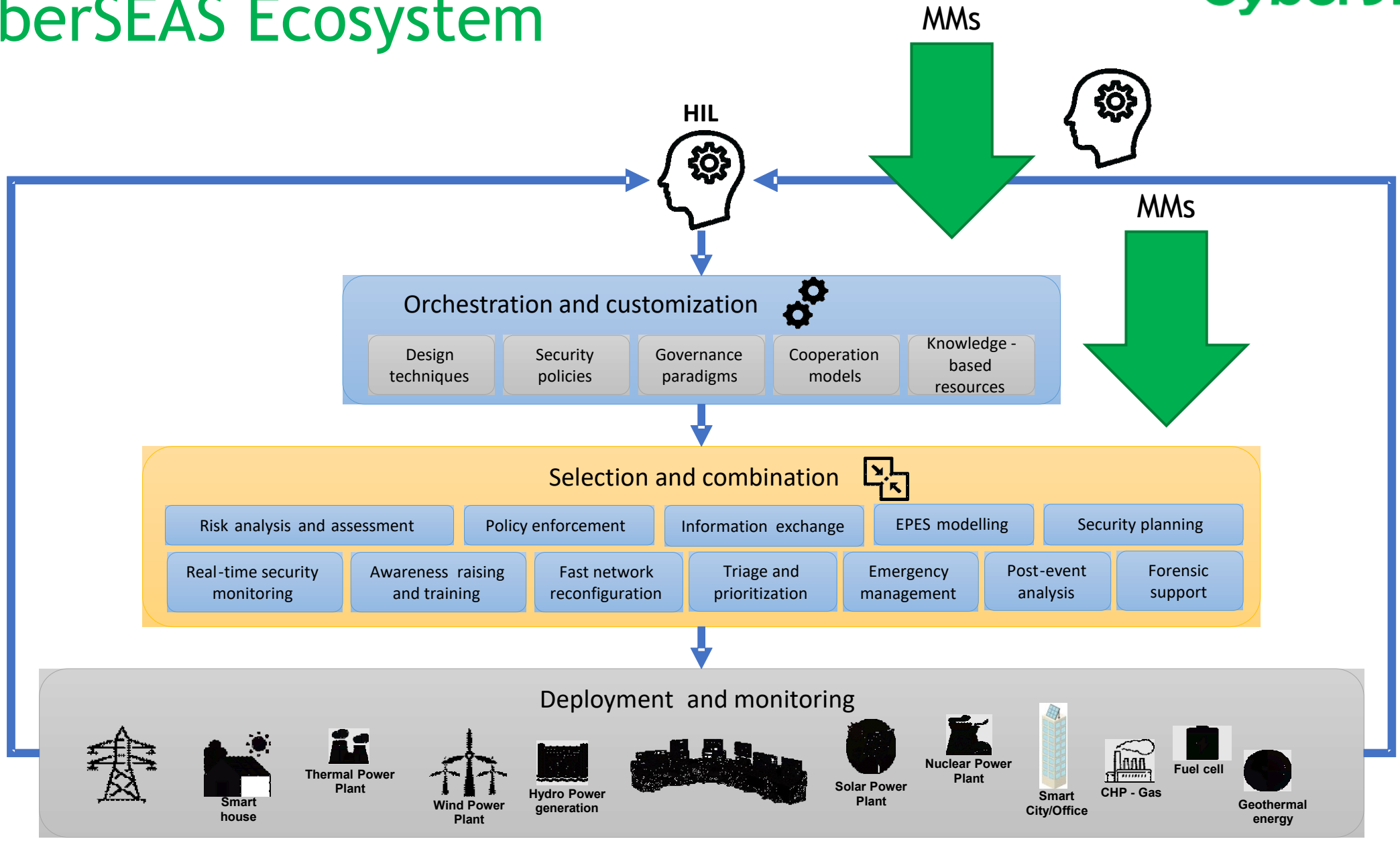


CyberSEAS Architecture



This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 101020560

CyberSEAS Ecosystem



This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 101020560

CyberSEAS Ecosystem

- ▶ A toolset of **30 security solutions**

- ▶ Deployable in pre-existing environments to take advantage of already deployed solutions



- ▶ An API and guidelines for selection and integration of COTS component to support a make or buy approach to infrastructure protection

- ▶ **57 commercial solutions analysed**



Validation Approach and Examples

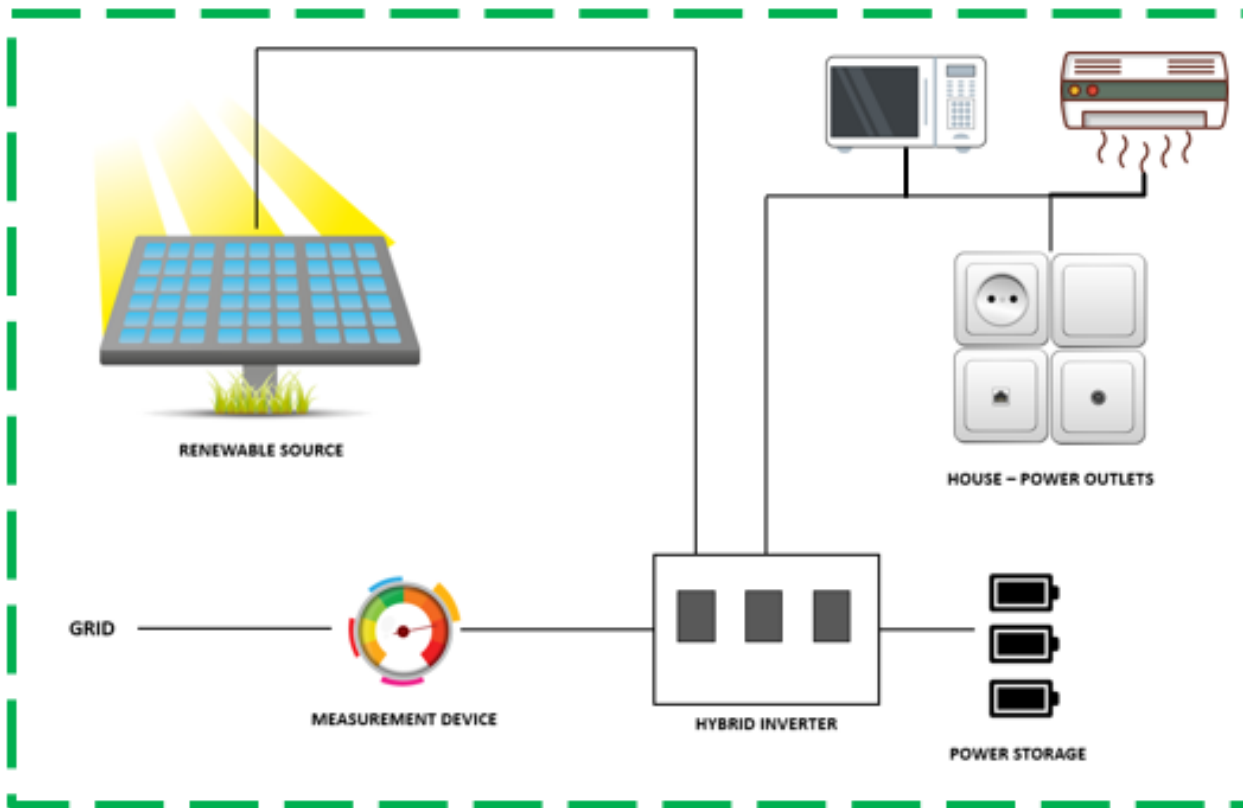
Six substantial infrastructures

- ▶ **Infrastructure 1 (Italy)**
 - ▶ Covers the distribution of electricity on medium and low voltage distribution networks for delivery to final customers, in two Italian municipalities (Benetutti and Berchidda)
- ▶ **Infrastructure 2 (Slovenia)**
 - ▶ Extends across the full chain and involves the most important energy domain players in the Slovenian electro-energy system
- ▶ **Infrastructure 3 (Croatia)**
 - ▶ Addresses the Main challenges of cross-stakeholder governance and service provisioning, in the context of a cross-border Croatia-Slovenia infrastructure
- ▶ **Infrastructure 4 (Finland)**
 - ▶ Focuses on a critical data exchange infrastructure which is not directly involved in the infrastructure for power production but directly impacts power production
- ▶ **Infrastructure 5 (Estonia)**
 - ▶ Fully automated power grid, where infrastructure operations must be protected from cyber attacks
- ▶ **Infrastructure 6 (Romania)**



This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 101020560

#1: Business Process IDS @ Berchidda



Focuses on: APT

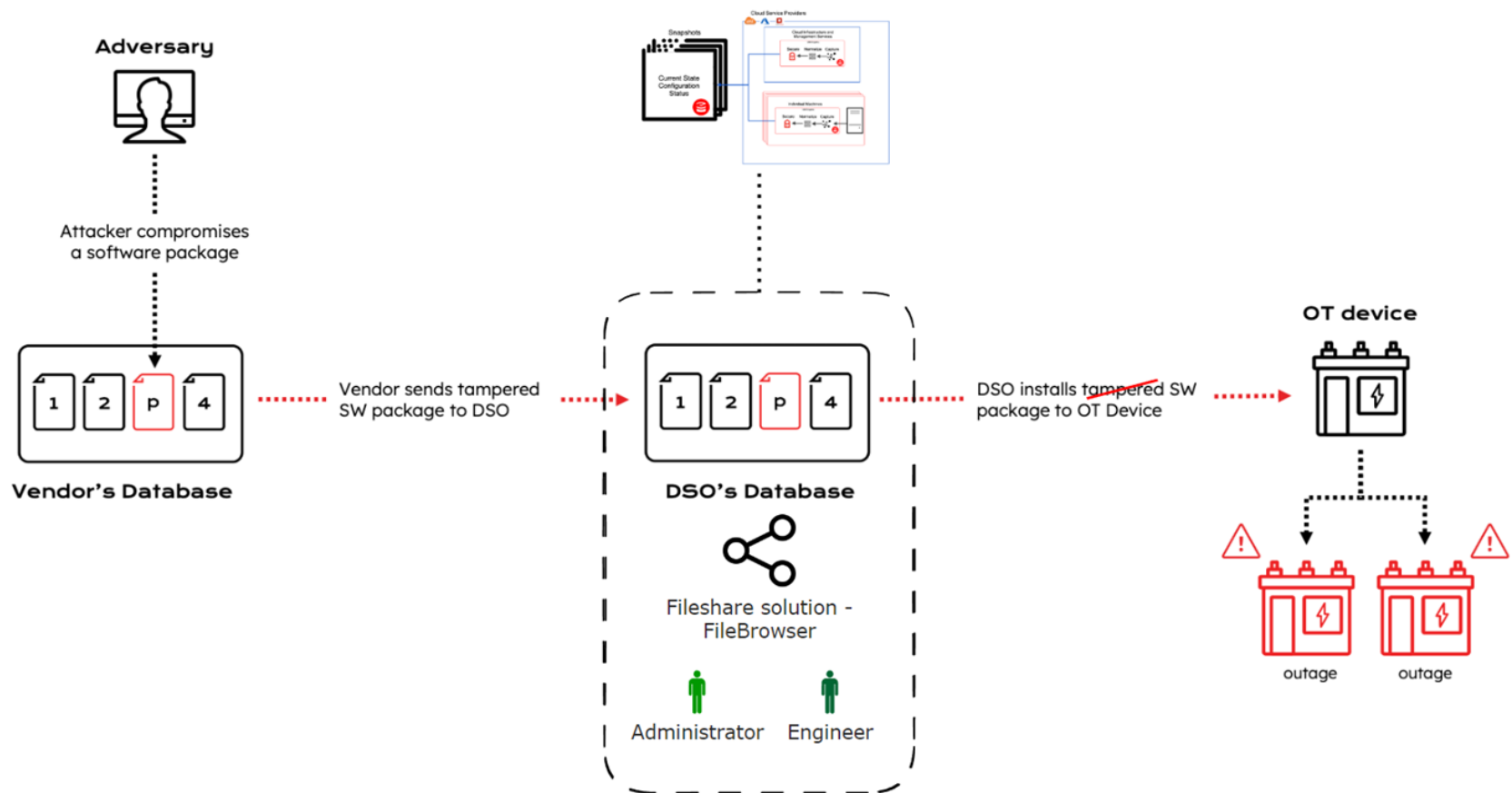
- A** ▶ **ADVANCED**
High Skills are required, and sophisticated techniques are used.
- P** ▶ **PERSISTENT**
Subtle, can be undetected for a long period of time.
- T** ▶ **THREAT**
Can lead to disruptive outcomes.

Covers:

SO#3



#2: MIDA tool @ ELEKTRILEVI



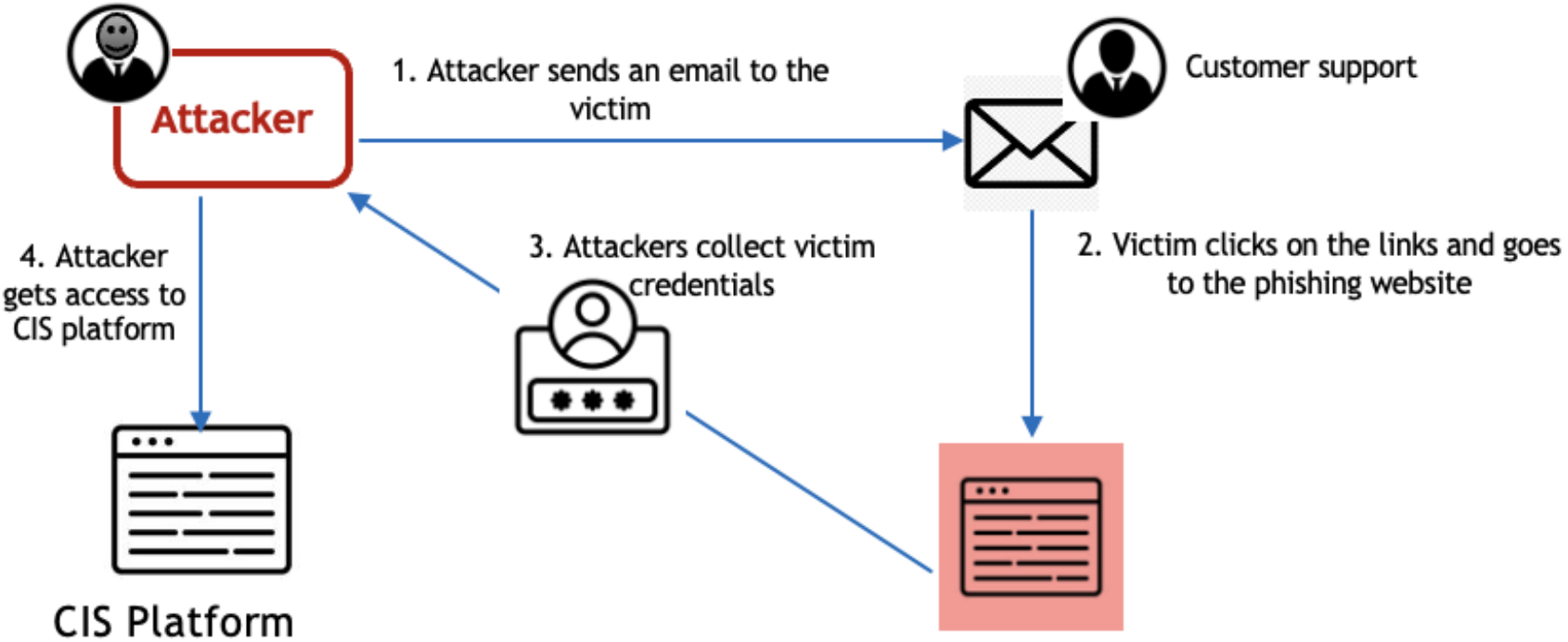
Focuses on:

- ➔ Tampered firmware updates

Covers:
SO#1



#3: ALIDA tool @ Finnish pilot



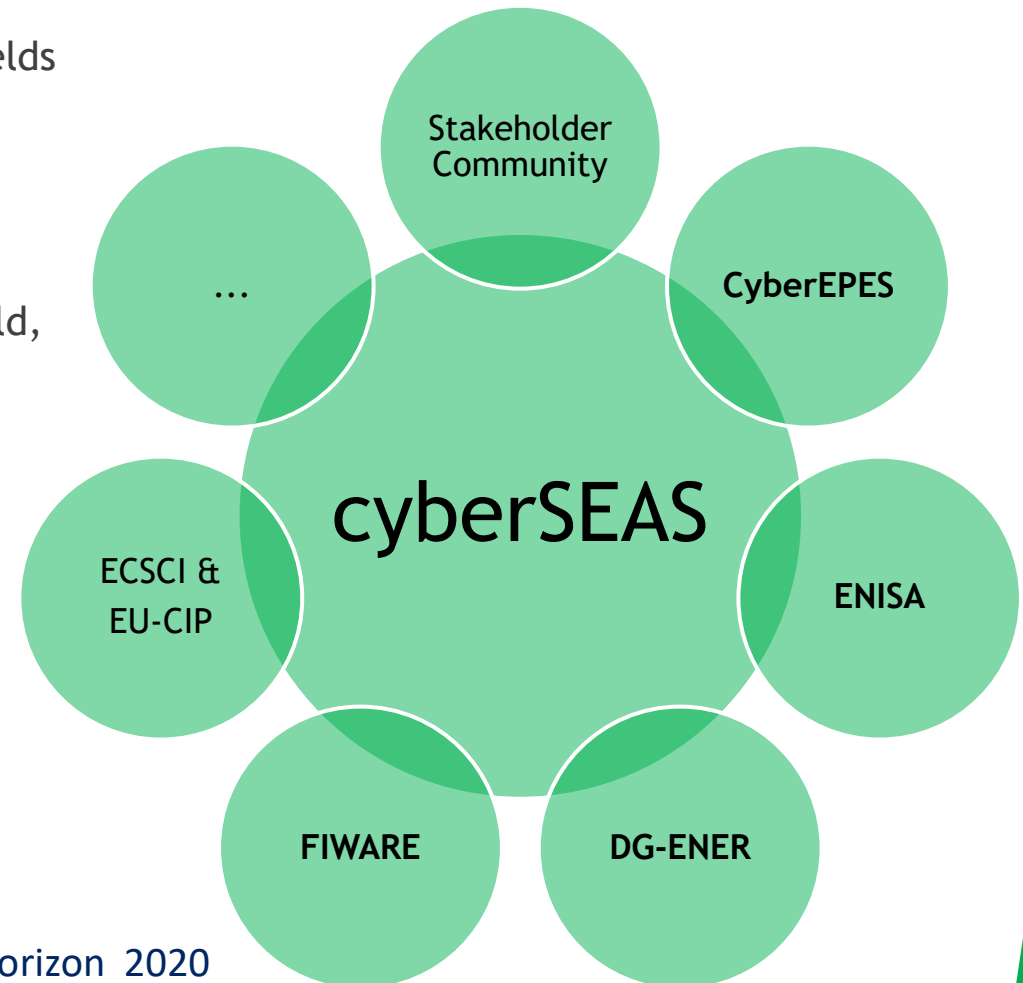
Focuses on:
Social Engineering attacks

Covers:
SO2 (including billing data)



Main Non-Technical Achievements

- ▶ **Creation and animation of the CyberSEAS stakeholders' community**
 - ▶ 45+ representatives from energy stakeholders & related fields
 - ▶ External validation of CyberSEAS results
- ▶ **Coordination of the CyberEPES cluster**
 - ▶ Cluster participants: PHOENIX, SDN-microsense, EnergyShield, ELECTRON, CyberSEAS, IRIS, IoTAC, AI4CYBER, DYNABIC
 - ▶ Promoting synergies (research topics, use cases, data)
- ▶ **Interaction with EU-level initiatives**
 - ▶ ECSCI cluster & EU-CIP
 - ▶ DG-ENER - interest in data privacy setup and consent management
 - ▶ ENISA - alignment meeting
 - ▶ FIWARE - organisation of FIWARE bootcamp 5-9/06/2023 & Global Summit



Our web contacts



<https://cyberseas.eu>

<https://cyberseas.eu/cyberepes/>



<https://www.linkedin.com/company/cyberseas-project>



<https://www.facebook.com/Cyberseas>



https://twitter.com/cyberseas_eu



Thank you!



Paolo Roccetti
(paolo.roccetti@eng.it)

