TEAM UPDATE
PLANNED ACTIVITIES IN 2023

• Tier 1 support
• Phishing automation and publicly available blocklists (+ CNW WG initiative)
• Support of nuclear cybersecurity via SNSA
• Support&training in Montenegro
• CyberSEAS partner
• NIS2 implementation
VARNI NA INTERNETU

- 10 years (steady financing)
- Activities thru the whole year
- ECSM coordination
- Varni v pisarni – Safe in the office
- Cooperation with stakeholders
  - Awareness raising of senior citizens: MOL, MDP
NIS2
"EXPLOSION" OF OBLIGEE

expands the circle of obligee (Article 2) to:

• in addition to the essential ones, also "important subjects"
• providers of public EC networks and publicly available EC services
• trust service providers
• top level domain name registries and domain name system service providers
• public administration entities at the central state and regional level
• entities that "register domain names, regardless of their size"

• introduces the term "near miss"
NATIONAL STRATEGY (ARTICLE 7)

• defines policies and other mandatory parts
• a mechanism for identifying the appropriate means
• vulnerability management
• education and training
• citizen awareness plan
• availability, integrity and confidentiality
• renewal at least every 5 years
(3.e) conducting, at the request of a material or significant entity, a proactive review of the network and information systems of that entity to detect vulnerabilities that could have a material impact;

(3) CSIRT groups may conduct proactive and unobtrusive inspections of publicly accessible network and information systems of essential and important entities. Such scanning is performed to detect vulnerable or unreliably configured network and information systems and to notify the relevant entities. Such screening must not have a negative impact on the operation of the entities' services.

(4) CSIRT groups cooperate with relevant stakeholders from the private sector to achieve the objectives of this directive.
VULNERABILITY DISCLOSURE (ARICLE 12)

• one CSIRT per MS is the coordinator
• tasks:
  • identification of relevant subjects and establishment of contact with them;
  • supporting natural or legal persons reporting vulnerabilities, and
  • negotiating timelines for disclosure and management of vulnerabilities affecting multiple entities.
• ENISA maintains a vulnerability register (has a copy of the CVE register)
HIGHLY CRITICAL SECTORS (PR. I)

1. energy (electricity, district heating and cooling, oil, gas, hydrogen)
2. transport (air, rail, water, road)
3. banking
4. financial market infrastructure
5. health
6. drinking water
7. waste water
8. digital infrastructure (IXP, DNS, ccTLD, cloud services, data centers, content delivery, trust services, public communication networks, publicly available services)
9. management of ICT services
10. public administration
11. space
OTHER CRITICAL SECTORS (PR. II)

• postal and courier services
• waste management
• manufacture, production and distribution of chemicals
• production, processing and distribution of foodstuffs
• production (medical and diagnostic devices, production of computers, electronic and optical products, electrical devices, other machines and devices, motor and other vehicles)
About the project

CyberSEAS at a glance

<table>
<thead>
<tr>
<th>Topic:</th>
<th>SU-D504-2018-2020 Horizon 2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grant Number:</td>
<td>101020560</td>
</tr>
<tr>
<td>Total Cost:</td>
<td>€ 10,067,121.25</td>
</tr>
<tr>
<td>EC Contribution:</td>
<td>€ 7,999,113.64</td>
</tr>
<tr>
<td>Start Date:</td>
<td>01/10/2021</td>
</tr>
<tr>
<td>End Date:</td>
<td>30/09/2024</td>
</tr>
</tbody>
</table>

CyberSEAS: improving the cyber security of the European Electrical Power and Energy Systems.
Strategic objectives

- SO1 - Countering the cyber risks related to the highest impact attacks against Electrical Power and Energy Systems (EPS)
- SO2 - Protecting consumers against personal data breaches and cyber attacks
- SO3 - Increasing security of the Energy Common Data Space (enhancing the governance relating to exchanging operational data across interconnected EPS)
Solutions

- CyberSEAS delivers an open and extendable ecosystem of 30 customisable security solutions providing effective support for key activities, and in particular:
  - risk assessment,
  - interaction with end devices,
  - secure development and deployment,
  - real-time security monitoring,
  - skills improvement and awareness,
  - certification, governance and cooperation.

- Out of the 30 solutions, 20 will reach TRL\textsuperscript{1}8+ (System complete and qualified) and 10 TRL\textsuperscript{1}7 (System prototype demonstration in operational environment).

\textsuperscript{1}TRL - Technology readiness level
## CyberSEAS solutions

<table>
<thead>
<tr>
<th>Provided by</th>
<th>Tool</th>
<th>Tool features/objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 ACS</td>
<td>CyberRange</td>
<td>Advanced simulation solution to easily model IT/OT systems composed of tens or hundreds of machines and simulate realistic scenarios including real cyber-attacks</td>
</tr>
<tr>
<td>2 CINI</td>
<td>ATRS</td>
<td>Advanced Tamper Resistant Storage</td>
</tr>
<tr>
<td>3 CINI</td>
<td>BP-IDS</td>
<td>Intrusion detection system acting based on business/process level KPIs</td>
</tr>
<tr>
<td>4 CINI</td>
<td>CI SOC</td>
<td>Advanced SOC with features dedicated to CIs</td>
</tr>
<tr>
<td>5 CINI</td>
<td>HwTEE</td>
<td>JNI-based bridge for Intel SGX TEE technology</td>
</tr>
<tr>
<td>6 CINI</td>
<td>PKI</td>
<td>High-performance secure enclave for cryptographic key management.</td>
</tr>
<tr>
<td>7 CINI</td>
<td>SIEM</td>
<td>Fully fledged SIEM solution with enhanced situation awareness capabilities</td>
</tr>
<tr>
<td>8 CINI</td>
<td>Virtual Testbed</td>
<td>Cyber-range training environment providing EPES users with a virtual SCADA setup</td>
</tr>
<tr>
<td>10 ENG SYN</td>
<td>ALIDA</td>
<td>Micro-service oriented platform for the composition, deployment and execution of Big Data Analytics (BDA) services implementing an extensive set of supervised and unsupervised machine learning algorithms</td>
</tr>
<tr>
<td>11 ENG</td>
<td>D.HUB</td>
<td>Digital Platform Services for secure hosting of managed EPES services</td>
</tr>
<tr>
<td>12 ENG</td>
<td>ESOC</td>
<td>Correlates events from cyber and physical sources / proposes intrusion responses using ML</td>
</tr>
<tr>
<td>13</td>
<td>ENG</td>
<td>IEC 62443-4-2</td>
</tr>
<tr>
<td>----</td>
<td>-----</td>
<td>---------------</td>
</tr>
<tr>
<td>14</td>
<td>ENG</td>
<td>OPENESS.edu</td>
</tr>
<tr>
<td>15</td>
<td>ENG</td>
<td>Situation picture dashboard and visual analytics</td>
</tr>
<tr>
<td>16</td>
<td>ENG</td>
<td>SSecA</td>
</tr>
<tr>
<td>17</td>
<td>ENG</td>
<td>RATING</td>
</tr>
<tr>
<td>18</td>
<td>ENG</td>
<td>T04SEE</td>
</tr>
<tr>
<td>19</td>
<td>Fraunhofer</td>
<td>Testing lab</td>
</tr>
<tr>
<td>20</td>
<td>Fraunhofer</td>
<td>SAPPAN Toolbox</td>
</tr>
<tr>
<td>21</td>
<td>GT</td>
<td>MID A</td>
</tr>
<tr>
<td>22</td>
<td>ICS</td>
<td>Penetration testing framework</td>
</tr>
<tr>
<td>23</td>
<td>IKE</td>
<td>Evaluation lab</td>
</tr>
<tr>
<td>24</td>
<td>IKE</td>
<td>Heindall</td>
</tr>
<tr>
<td>25</td>
<td>RWTH</td>
<td>Attack-Defence Simulator</td>
</tr>
<tr>
<td>26</td>
<td>SQS</td>
<td>SQS Test Lab</td>
</tr>
<tr>
<td>27</td>
<td>STAM</td>
<td>DAISY</td>
</tr>
<tr>
<td>28</td>
<td>STAM</td>
<td>KARMA</td>
</tr>
<tr>
<td>29</td>
<td>SYN</td>
<td>Federated Learning Framework</td>
</tr>
<tr>
<td>30</td>
<td>WINGS</td>
<td>ARTEMIS</td>
</tr>
</tbody>
</table>

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

- **CyberSEAS solutions will be validated** through experimental campaigns consisting of 100+ attack scenarios.
- The pilot scenarios will be reproduced in **lab for a preliminary evaluation of CyberSEAS features and tools**. (Labs: Ikerlan, Software Quality Systems, Fraunhofer FIT and RWTH Aachen University).
- And after their final tuning the scenarios will be deployed in one of the **6 infrastructures provided by CyberSEAS partners**
  - Estonia
  - Finland
  - Italy
  - Romania
  - Slovenia+Croatia
Slovenian-Croatian pilot project

- Challenges of continuous and uninterrupted collection of non-energy related data.
  - ELES and OPERATO collect and use environmental data from different sources to optimize network power flows close to real time using novel system for dynamic line rating called SUMO. This data automatically feeds SUMO that is connected with SCADA systems supporting real time system operation.

- Challenges of cooperation between TSO's, aggregators, retailers and diverse prosumers, when using public communication networks.
  - It addresses cyber-security challenges of current energy-domain data exchanges using economically favourable (public) communication connections compliant to technical standards and propose new means of secure communications supporting wide cooperation with aggregators as well as open governance solutions for cooperation. It connects with the Slovenian CERT.

- Challenges of cyber-security governance across organisations
  - extending to the national agencies and CERT.

- Challenges of cross-border cooperation among Slovenian and Croatian TSO (HOPS).
  - The campaign will use the MeliCERTs platform/tools, with partner SI-CERT. It will also address structural data exchange between Eles and HOPS for the needs of the Virtual Cross-border Control Center.

¹TSO – Transmission system operator
### Slovenian-Croatian pilot project's topics

<table>
<thead>
<tr>
<th>PARTNER</th>
<th>Topic 1 (Securing energy and non-energy data exchanges)</th>
<th>Topics 2 (Cyber-security cooperation scenarios / governance model)</th>
<th>Topic 3 (Cyber-security cooperation scenarios / governance model / Cross-border)</th>
<th>Main asset related to the pilot project</th>
</tr>
</thead>
<tbody>
<tr>
<td>ELES (Slovenian TSO) OPERATIO (Doughter company of ELES)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Transmission power system, SCADA/EMS, Balancing Services Market Platform, SUMO Dynamic Rating system, Sincro.grid VCC</td>
</tr>
<tr>
<td>HOPS (Croatian TSO)</td>
<td>X</td>
<td></td>
<td>X</td>
<td>Transmission power system, Sincro.grid VCC</td>
</tr>
<tr>
<td>PETROL</td>
<td>X</td>
<td>X</td>
<td></td>
<td>Distributed energy resources, Ve.TER Virtual Power Plant platform</td>
</tr>
<tr>
<td>INFORMATIKA</td>
<td>X</td>
<td>X</td>
<td>(X)</td>
<td>SOC</td>
</tr>
<tr>
<td>SI CERT</td>
<td>X</td>
<td></td>
<td>X</td>
<td>MelICERTes platform</td>
</tr>
<tr>
<td>ICS</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Penetration testing equipment</td>
</tr>
</tbody>
</table>
Exchange of feeds, events and incidents

- Indicators of compromise (IoC)
- Cyber Threat Intelligence (CTI)

1 DSO – Distribution system operator
2 BSP – Balancing service provider
Exchange of feeds, events and incidents

- Indicators of compromise (IoC)
- Cyber Threat Intelligence (CTI)

TSO ELES

SOC for Slovenian DSOs

TSO HOPS

MeliCERTes platform

SI-CERT

CERT.HR
Stakeholders welcome

- Be informed about main projects processes and technical developments in the area of EPES
- Possibility for exchanging best practices and latest experiences in EPES environment
- Possibility to influence on preparation of new EU regular framework in the area of EPES with proposals and suggestions
- Possibility to influence on preparation of new standardization framework in the area of EPES with proposals and suggestions
- Become an important part of the expert network for sharing new security-related ideas in the EPES area
Thank you!

Matej Breznik
SI-CERT
matej.breznik@cert.si