D8.2

Report on stakeholder community building and clustering with relevant projects and initiatives – ver.2

DOCUMENT	D8.2	**WORKPACKAGE**	WP8
DELIVERABLE STATE	Final	**PROGRAMME IDENTIFIER**	H2020-SU-DS-2020
REVISION	V1.0	**GRANT AGREEMENT ID**	101020560
DELIVERY DATE	30/09/2024	**PROJECT START DATE**	01/10/2021
DISSEMINATION LEVEL	PU	**DURATION**	3 YEARS

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

DISCLAIMER

This document does not represent the opinion of the European Commission, and the European Commission is not responsible for any use that might be made of its content.

This document may contain material, which is the copyright of certain CyberSEAS consortium parties, and may not be reproduced or copied without permission. All CyberSEAS consortium parties have agreed to full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the CyberSEAS consortium as a whole, nor a certain party of the CyberSEAS consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and does not accept any liability for loss or damage suffered using this information.

ACKNOWLEDGEMENT

This document is a deliverable of CyberSEAS project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101020560.

The opinions expressed in this document reflect only the author's view and in no way reflect the European Commission's opinions. The European Commission is not responsible for any use that may be made of the information it contains.

PROJECT ACRONYM	CyberSEAS
PROJECT TITLE	Cyber Securing Energy dAta Services
CALL ID	H2020-SU-DS-2020
CALL NAME	Digital Security (H2020-SU-DS-2018-2019-2020)
TOPIC	SU-DS04-2018-2020 Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches
TYPE OF ACTION	Innovation Action
COORDINATOR	ENGINEERING – INGEGNERIA INFORMATICA SPA (ENG)
PRINCIPAL CONTRACTORS	CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA (CINI), AIRBUS CYBERSECURITY GMBH (ACS), FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (FRAUNHOFER), GUARDTIME OU (GT), IKERLAN S. COOP (IKE), INFORMATIKA INFORMACIJSKE STORITVE IN INZENIRING DD (INF), INSTITUT ZA KORPORATIVNE VARNOSTNE STUDIJE LJUBLJANA (ICS), RHEINISCH-WESTFAELISCHE TECHNISCHE HOCHSCHULE AACHEN (RWTH), SOFTWARE IMAGINATION & VISION SRL (SIMAVI), SOFTWARE QUALITY SYSTEMS SA (SQS), STAM SRL (STAM), SYNELIXIS LYSEIS PLIROFORIKIS AUTOMATISMOU & TILEPIKOINONION ANONIMI ETAIRIA (SYN), WINGS ICT SOLUTIONS INFORMATION & COMMUNICATION TECHNOLOGIES IKE (WIN), ZIV APLICACIONES Y TECNOLOGIA SL (ZIV), COMUNE DI BERCHIDDA (BER), COMUNE DI BENETUTTI (BEN), ELES DOO SISTEMSKI OPERATER PRENOSNEGA ELEKTROENERGETSKEGA OMREZJA (ELES), PETROL SLOVENSKA ENERGETSKA DRUZBA DD LJUBLJANA (PET), AKADEMSKA RAZISKOVALNA MREZA SLOVENIJE (ARN), HRVATSKI OPERATOR PRIJENOSNOG SUSTAVA DOO (HOPS), ENERIM OY (ENERIM), ELEKTRILEVI OU (ELV), COMPANIA NATIONALA DE TRANSPORT ALENERGIEI ELECTRICE TRANSELECTRICA SA (TEL), CENTRUL ROMAN AL ENERGIEI (CRE), TIMELEX (TLX).
WORKPACKAGE	WP8
DELIVERABLE TYPE	**R Document, report** DEM Demonstrator, pilot, prototype DEC Websites, patent fillings, videos, etc. OTHER ETHICS Ethics requirement ORDP Open Research Data Pilot DATA data sets, microdata, etc.
DELIVERABLE TYPE	Report
DISSEMINATION LEVEL	**PU Public** CO Confidential, only for members of the consortium (including the Commission Services) EU-RES Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)

	EU-CON Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC) EU-SEC Classified Information: SECRET UE (Commission Decision 2005/444/EC)
DELIVERABLE STATE	FINAL
CONTRACTUAL DATE OF DELIVERY	30/09/2024
ACTUAL DATE OF DELIVERY	30/09/202454
DOCUMENT TITLE	Report on stakeholder community building and clustering with relevant projects and initiatives – ver.2
AUTHOR(S)	Ziga Podgorsek, Eva Caleta, Denis Caleta (ICS)
REVIEWER(S)	SIMAVI, CRE
ABSTRACT	SEE EXECUTIVE SUMMARY
HISTORY	SEE DOCUMENT HISTORY
KEYWORDS	EPES, Stakeholder Community, Clustering, cyber security, collective intelligence

Document History

Version	Date	Contributor(s)	Description
V0.1	15/08/2024	ICS	1st Draft
V0.2	26/08/2024	ICS	2st Draft
V.03	31/08/2024	SIMAVI, CRE	Review
V.04	15/09/2024	ICS	Pre final version
V1.0	16/09/2024	ICS, ENG	Final version

Table of Changes in Version 2

Section	Contributor	Chenge description and motivation
1.	ICS	In the introduction, new introductory information has been added related to the activities during the entire duration of the project and links to the content of the report in version 1.
2.	ICS	In chapter 2, new methodological frameworks were added, which are aimed at the operation and activities of the second period of the project. The content is meaningfully connected to the whole together with the basics that were defined in the first version of the report.
3.	ICS	In chapter 3, new content related to important additional target groups, which proved to be relevant for the project in the second half of the project's duration, was sensibly added.
5.	ICS + technology partners + pilot partners	This chapter has been completely upgraded and the content has been greatly improved. The chapter reflects the main content points and results of the work in the second part of the project, which are based on detailed interviews, a detailed report of the review of activities within the CyberSEAS Stakeholder Group. The main findings of good practices and added values brought by various forms of cooperation of the CyberSEAS project with other initiatives and related projects are added. The results through the achievement of the set KPIs are also presented in detail.
6.	ICS	In the conclusion, additional activities and integrated content of the conclusion are logically summarized for the duration of the entire period of the task T8.1.

Table of Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

AKOS	Communications Networks and Services Agency of the Republic of Slovenia
AHP	Analytical Hierarchical Process
CIP	Critical Infrastructure Protection
CL	Cascading Level
CEI	Critical energy infrastructure
CEIS-SG	Critical Energy Infrastructure Security Stakeholders Group
CIRTS/ CERTS	Computer emergency response team
CoU	Community of Users
ECSO	European Cybersecurity Organization
DER	Distributed Energy Resources
DG ENER	Directorate-General for Energy
ECCC	European Competence Network of Cybersecurity Centres
ENISA	The European Union Agency for Cybersecurity
ENTSO-E	European Network of Transmission System Operators for Electricity
EPES	Electrical Power and Energy System
EE-ISAC	European Energy – Information Sharing & Analysis Centre
ECSCI	European Cluster for Securing Critical Infrastructure
IDSA	International Data Spaces Association
IED	Intelligent Electronic Device
IM	Information Management
KPI	Key performance indikator
PES	Power and Energy System
PLC	Programmable Logic Controller
REA	Research European Agency
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition

SGAM	Smart Grid Architecture Model
SODO	Electricity distribution system operator
SOTA	State of the art analyses
TNCEIP	Thematic Network on Critical Energy Infrastructure Protection
VS	Vulnerability Score
WP	Work Package

Executive Summary

This deliverable outlines the finalizing and execution of strategy and activities for establishing the CyberSEAS Stakeholder Community and for clustering with other relevant projects and initiatives. It provides clear evidence of the operating and building a robust Stakeholder Community, including identifying various dissemination channels for the exchange of collective intelligence. The report D8.1 offered a detailed analysis of ongoing projects and initiatives, identifying potential connection points and opportunities for collaboration. The latter part of the initial report presented a plan and actionable steps for building an extensive network of operators, with the capacity to integrate external project outcomes into this network. The creation of the Stakeholder Community and the identification of clustering opportunities have been closely linked to the development of strategies and activities for dissemination within the CyberSEAS project, highlighting the importance of close collaboration with scientific and professional communities in the EPES sector.

This D8.2 report builds upon and significantly extends the groundwork laid in the D8.1 report, which initially set the planning foundations for the establishment of the CyberSEAS Stakeholder Community and also framework for clustering with other relevant projects and initiatives, forming the strategic backbone of the CyberSEAS project's outreach and collaboration efforts.

In this final iteration of the report, we delve deeply into the concrete activities that were executed over the course of the project. These activities represent the culmination of extensive and coordinated efforts by the project partners, aiming to foster a vibrant and engaged stakeholder community. The report meticulously documents the outcomes of these efforts, providing a comprehensive account of the technological advancements and process improvements achieved.

Moreover, the report emphasizes the key findings derived from a series of quantitative and qualitative studies, surveys, and inquiries. These were conducted with active participation from the CyberSEAS Stakeholder Community and were instrumental in guiding the project’s trajectory. The feedback gathered through these channels provided critical insights that informed the adaptation and refinement of the project’s technological and process solutions. These adjustments ensured that the project outcomes were not only aligned with but also highly responsive to the real-world needs of the EPES (Electrical Power and Energy Systems) environment.

This report also introduces new chapters and content that were not present in the D8.1 report. These additions are clearly marked to distinguish them from the foundational information presented earlier. By doing so, readers can easily identify the innovations and developments that have emerged in the latter stages of the project. The new sections provide updated insights and reflections on the progress made, the challenges encountered, and the strategies employed to overcome them.

Additionally, the report addresses the sustainability of the CyberSEAS Stakeholder Community and its activities beyond the project’s official timeline. It outlines the steps taken to ensure

that the collaborations, knowledge exchange, and community building efforts initiated during the project will continue to evolve and flourish. This forward-looking approach underscores the project's commitment to fostering a long-term culture of cyber-resilience within the EPES sector.

In summary, this D8.2 report not only serves as a comprehensive documentation of the activities and achievements of the CyberSEAS project but also as a strategic guide for sustaining and expanding the impact of these efforts in the future. The report's detailed account of the new chapters, combined with the analysis of key findings and the emphasis on post-project sustainability, makes it an essential resource for stakeholders involved in the ongoing development of cyber-resilient energy systems.

1 Introduction

To ensure efficient and secure functioning of modern day grid, there has been an increased need for interactions between stakeholders, exchange of data, new policies, new knowledge and best practices. One of the key objectives of the CyberSEAS project is to focus on the creation of a strong stakeholder community. To build such strong stakeholder networks with related exchanging processes and procedures we need to create a strong base for a common understanding that the secure operation of EPES organizations in the challenging international environments should be based on efficient collecting, exchanging, and processing of new knowledge on EPES environments. Study material, best practices, new technical developments, factsheets, and guidelines related to cyber-physical protection of EPES will be created through CyberSEAS project and provided also to CyberSEAS Stakeholder Community. The next important part of task 8.1 is focused on clustering and cooperation with relevant projects and initiatives. We are facing different research and innovative projects and initiatives inside and outside of EU which are focused on different aspects of providing comprehensive security approaches for securing EPES operational environment. This deliverable provides a detailed analysis of ongoing projects activities which could be performed and may form connection points for further exploitation of common approaches and results. These two main processes inside this task provided an efficient base for a wide operator network which was fed with the project's results.

The design and implementation of the material blended cyber and physical aspects in an integrated EPES security operational process. The material was available throughout a Stakeholder community network which has been developed in the framework of the project. Through this network we provided and continuously support interactions, exchange, and bottom-up co-creation of practices, sharing of experience and knowledge. This has become a regular base for exchanging relevant information among different internal and external members of the network called CyberSEAS Stakeholder Community.

This is the reason for proper understanding definition and processes of collective intelligence and the creation of CyberSEAS Stakeholder Community. We also provided some important definitions and approaches to these processes.

Persons and expert communities are becoming important sources of knowledge, well beyond traditionally known boundaries. This situation entails opportunities for tapping into and benefiting from such available knowledge – often termed as *collective intelligence* – for co-creation and building solutions to security problems faced by individuals, organizations and expert societies.

Collective intelligence (CI) is shared or group intelligence that emerges from the collaboration, collective efforts, and competition of many individuals and appears in consensus decision making. Currently, the EU's innovation concept [1] is defined as the adoption of new products, processes, marketing, or organizational approaches that create a valuable outcome in terms of financial benefit, well-being, or efficiency. It is a holistic approach to innovation, as it incorporates the use of existing technologies in new applications as well as non-technological and social innovation. This is also related to the innovation approach in the area of critical infrastructure protection with special focus on EPES operational environment. This concept entails new ideas (products, services, and models) that simultaneously meet needs, target environments in critical infrastructure (more effectively than the alternatives) and create new social relationships or forms of collaboration. Its social aspect refers to both its content and process. In terms of content, it aims primarily to meet security needs in comprehensive protection of critical infrastructure against physical, cyber and human threats while providing an appropriate level of resilience. In terms of process, it often entails broad participation, engagement, empowerment, co-design and bottom-up sharing or grassroots security and safety initiatives. With technological development, this empowerment becomes stronger, which makes it easier for experts from target EPES environments to participate in collective problem solving through co-creating, co-designing, and co-evaluating security policies, processes, services and new technology innovations.

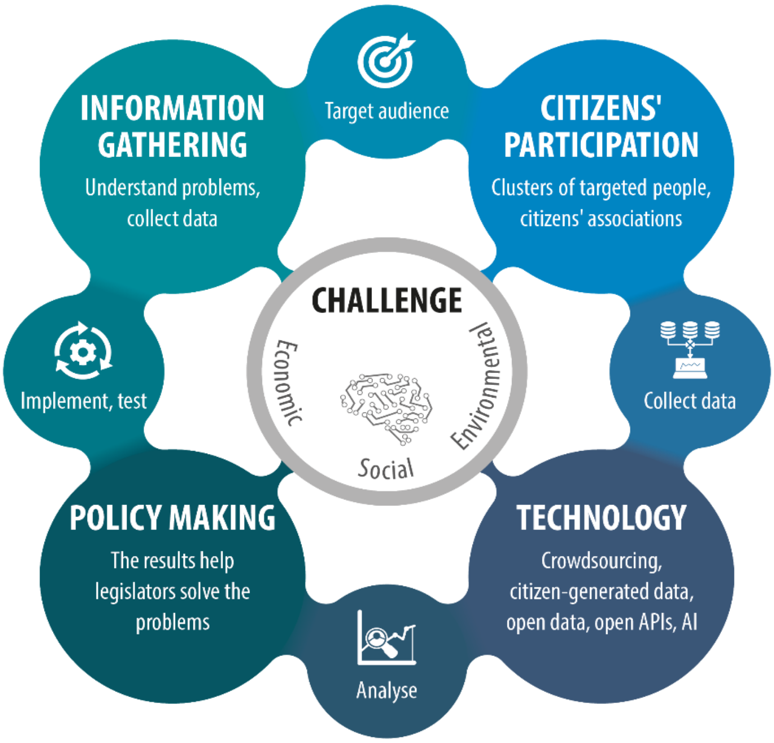

INFORMATION GATHERING
Understand problems, collect data
Target audience
CITIZENS' PARTICIPATION
Clusters of targeted people, citizens' associations
Implement, test
CHALLENGE
Economic
Environmental
Social
Collect data
POLICY MAKING
The results help legislators solve the problems
Analyse
TECHNOLOGY
Crowdsourcing, citizen-generated data, open data, open APIs, AI

Figure 1: Representation of the main elements of collective intelligence for solving challenges in society [2].

The EU is promoting social innovation dialog through "collective intelligence networks" [3]. A stakeholder network can be designed to promote a particular view on an issue, exchange knowledge, and solve problems. Collective intelligence can be harnessed and directed through the Stakeholder community. They can empower groups and impact collective security behavior if they are open, flexible, and dynamic. Their success depends greatly on self-organization, transparency, trust, motivation, and a balance among participants' individual goals. This has provided the motivation for the inclusion of the CyberSEAS Stakeholder community, which is presented in the following chapters and enables an efficient framework for collecting and exchanging all relevant information, best practices and new knowledge related to EPES among members of this network. This shows that in basic this cooperation among the members of CyberSEAS Stakeholder Community is expected in two directions and it is not solely focused on relation to CyberSEAS result's sharing towards the community. An important part also represents the bottom-up approach where we will collect important and valuable information which could strongly improve work in CyberSEAS project and of course strengthen the Stakeholder Community.

In the past, we have witnessed various initiatives to establish and operate networks and stakeholder communities for the exchange of experience, good practices and lessons learned. As a result, in the CyberSEAS project, we are aware of the possible risk that the establishment of a CyberSEAS Stakeholder Community would lead to another association/initiative that would further fragment attempts to find synergies between different initiatives and working links. For this reason, we wish to place the development of the CyberSEAS Stakeholder Community within the framework of existing initiatives, thereby adding an important part of new lessons that will be directed to the EPES area and, due to its applicability, also applicable to other critical infrastructure sectors. The direction of integration with other initiatives and projects will be further elaborated below.

Additionally, the use of *collective intelligence* is not just limited to day-to-day organizational work, but the ad hoc project-based work can benefit even more from the use of *collective intelligence* as project organizations have greater flexibility and lever to tap into knowledge beyond project organization boundaries.

1.1 Relation to other project activities

This Section indicates the connecting points and correlation with other tasks inside the project CyberSEAS. In order to effectively implement the planned activities of the establishment and operation of the CyberSEAS Stakeholder Community, it is necessary to understand in great detail the connections that individual parts of the CyberSEAS project have in the establishment of this network. The implementation of this task was closely related to all parts of the project, where the implementation of the activity brings new results in the field of processes, standards, new technologies and direct experience, which the partners achieved mainly through the implementation of pilot processes of testing developed technologies. Because of the above, the CyberSEAS Community activity mentioned have been closely related to the activities in WP2-WP9. It have been also necessary to ensure adequate coordination between the activities of the CyberSEAS Stakeholder Community and the operation of the WP9, which dedicated to the processes of exploitation, dissemination, and communication. This coordination was even more important from the point of view of preventing specific duplication of activities and, above all, creating synergies between the two processes.

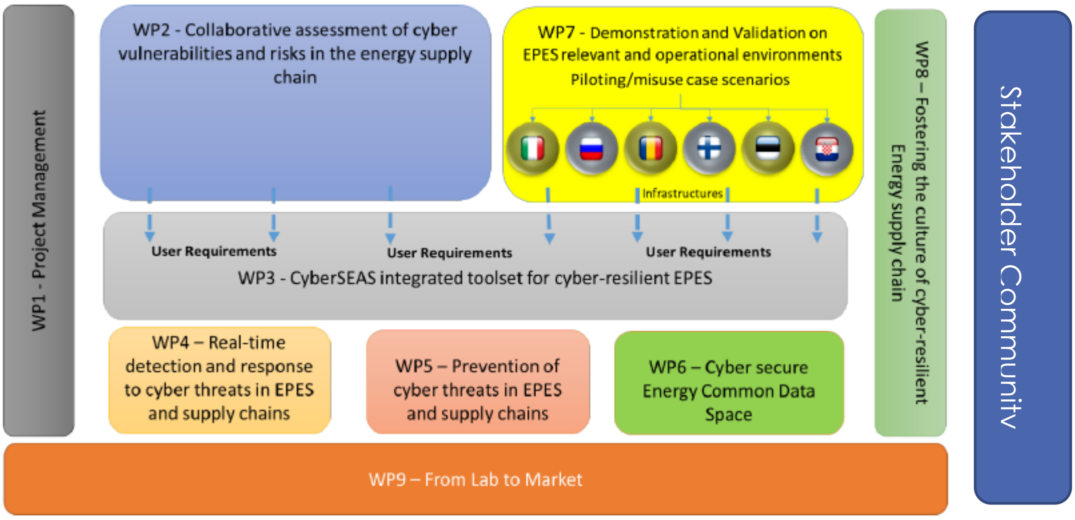

WP1 - Project Management
WP2 - Collaborative assessment of cyber vulnerabilities and risks in the energy supply chain
WP7 - Demonstration and Validation on EPES relevant and operational environments
Piloting/misuse case scenarios
Infrastructures
User Requirements
User Requirements
User Requirements
WP3 - CyberSEAS integrated toolset for cyber-resilient EPES
WP4 – Real-time detection and response to cyber threats in EPES and supply chains
WP5 – Prevention of cyber threats in EPES and supply chains
WP6 – Cyber secure Energy Common Data Space
WP8 – Fostering the culture of cyber-resilient Energy supply chain
WP9 – From Lab to Market
Stakeholder Community

Figure 2: CyberSEAS Stakeholder Community relations with other project activities

The creation of the Stakeholder Community and clustering opportunities were closely connected with developing strategy and activities in the dissemination of the CyberSEAS project. This is important due to close collaboration with scientific and professional communities in EPES area. Further synergies have been even more visible in joint work of these processes including management and exploitation.

CyberSEAS consortium succeed to properly build the stakeholder community reaching the no. of +100 stakeholders. Moreover, that there was a very efficient collaboration at the consortium level and synergies were exploited with the activities belonging to WP9, CyberSEAS Market Interest Group actively contributing both to the construction of the stakeholder community and to stakeholder engagement, through meetings, consultations and feed-back collection, to foster support for the project results.

2 Building the Stakeholder Community (UPDATED)

2.1 Vision and Goals

The vision of CyberSEAS project is to foster and support the creation of a culture of cyber security focusing on EPES as an important part of the critical infrastructure environment. Thus, the CyberSEAS **consortium** proposed the creation and management of the CyberSEAS Stakeholder Community, whose members are mainly EPES representatives, but also other practitioners involved in specific CIP and resilience, researchers and technologists standardization bodies, civil protection, first responders, and civil society. This group also represents wider audiences for disseminating project results.

We expected that the CyberSEAS Stakeholder Community members were the main target (responders and contributors) of relevant network. Of course, we cannot forget project partners and their role in this community.

Primarily goals were organization specific workshops during the project to disseminate the results to relevant communities of EPES and other stakeholders (also external to the CyberSEAS Stakeholder Groups) as well as relevant information on threats and vulnerabilities for EPES and information sharing methods and tools proposed by CyberSEAS. Moreover, it should be noted that the CyberSEAS Stakeholder community network was co-create the relevant knowledge on cyber security in EPES operational environment and made this information available also to a wide user community. To this, it is necessary to add an additional quality, which was represented by cooperation and the synergistic effect of joint activities with related projects and initiatives.

This task leads to the creation of a strong communication channel for exchanging study material, best practices factsheets, and guidelines related to the cyber-physical protection of EPES. The design and implementation of the material would blend cyber and physical aspects into an integrated body of knowledge. The CyberSEAS material has been made available throughout this network community supporting interactions, exchange, bottom-up co-creation of practices, sharing of experience and knowledge.

It is important to have clear target goals (KPI's) which we wanted to achieve through creation of CyberSEAS Stakeholder Community. The main KPI for this task were:

- 50 energy stakeholders external to the consortium taking up the CyberSEAS governance and cooperation support mechanisms to actively participate to information exchange (i.e. access/provide security related information on 3+ occasions each (on average)).
- Working groups involvements (e.g. ECSO WG's, BRIDGE WG etc.) establishing links with 6 initiatives such as European Energy – Information Sharing & Analysis Centre (EE-ISAC),

Thematic Network on Critical Energy Infrastructure Protection (TNCEIP), etc. – 15 references to work produced in CyberSEAS.

There were some additional KPI's which will be also supported by CyberSEAS Stakeholder Group and the existing operator network:

- 15 grid operators external to the consortium using CyberSEAS risk self-assessment evaluation features and rating them as superior to currently available offerings.

Support key dissemination objectives and goals:

- Increase cyber security awareness among consumers and prosumers;
- Increase collaboration between energy operators and connected infrastructures;
- Collaboration among energy operators;
- Connect to policy authorities and European agencies, CERTs and CSIRTs networks.

Table 1 Details the timeframe of the project phases:

Tools/channel	**KPIs**	**When**
Working groups involvements (e.g. ECSO WGs, BRIDGE WGs etc), establishing links with initiatives (European Energy – Information Sharing & Analysis Centre (EE-ISAC), Thematic Network on Critical Energy Infrastructure Protection (TNCEIP)	Target: 15 references to work produced in CyberSEAS across at least 5 initiatives	M12-M36
Brokerage events, public events, fairs participation: - Collaboration with other EU projects/initiatives - Local workshops at pilots' premises - Participation in relevant conferences (European Smart Grid Cyber Security, INCOSE conference in Israel, Electricity conference (IEEE), CyberEurope exercise month (ENISA))	Target: participation in 15 conferences (note: this target includes also participation depending on the COVID situation)	M1-M36
Project Leaflet Promotional material / electronic format	Target (from M12) 500 contacts to send to	First publication by M6 Quarterly updates

Table 1: List of KPI's connected to T8.1

2.2 Creating Stakeholder Community - Methodology and Procedures

The creation of Stakeholder Community is divided into four important supportive pillars. These pillars also represent the main contributors but also consumers of information related to the development of CyberSEAS project. These pillars were

- Members from CyberSEAS partner organizations;
- Members of organizational structure which support the CyberSEAS consortium (Members of Internal Advisory Board);
- CyberSEAS Market Interest Group (MIG);
- Related cyber security and critical infrastructure projects and initiatives connected with CyberSEAS project;
- Other Community of target organizations (Community of Users and EPES network operators, standardization or regulatory bodies and other relevant organizations)

All organizations and possible partner initiatives were elaborated in detail in the following chapters.

The main coordination of activities in Stakeholder Community were conducting by coordination committee, which is structured by the Project Coordinator, Technical Manager, Scientific Manager, Innovation Manager, and WP leaders, Advisory Board representative and T8.1. leader as an operational leader of stakeholder community.

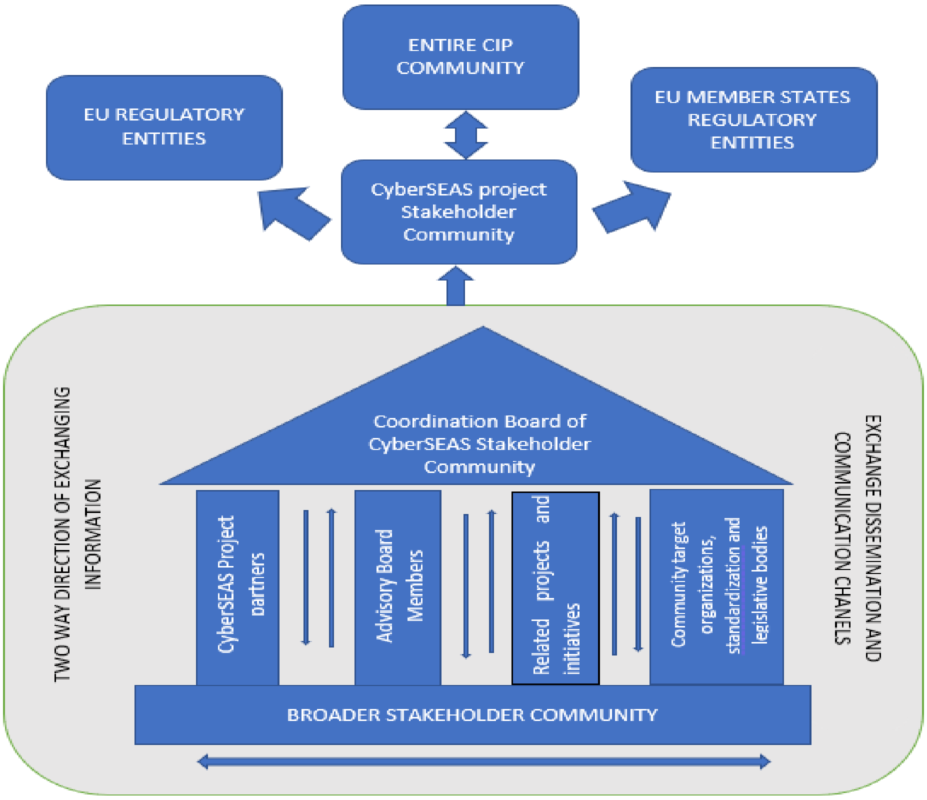

ENTIRE CIP COMMUNITY
EU REGULATORY ENTITIES
EU MEMBER STATES REGULATORY ENTITIES
CyberSEAS project Stakeholder Community
TWO WAY DIRECTION OF EXCHANGING INFORMATION
Coordination Board of CyberSEAS Stakeholder Community
CyberSEAS Project partners
Advisory Board Members
Related projects and initiatives
Community target organizations, standardization and legislative bodies
EXCHANGE DISSEMINATION AND COMMUNICATION CHANELS
BROADER STAKEHOLDER COMMUNITY

Figure 3: Organizational and procedural scheme of creation CyberSEAS Stakeholder Community

CyberSEAS Stakeholder Community is a network base and exchange communication channel for all participant organizations and individual EPES experts who were part of this exchange and cooperation community. The specific Collaborative and Knowledge Sharing services featured in the collaborative environment are the Basic Services and Social Collaboration Services.

Process for using collective intelligence [3] in CyberSEAS Stakeholder Community (main steps):

(1) Provide skills/training to project managers, project task leads and other participants

Organizations need to provide training and upskill the knowledge of key people including project managers, task leaders and focal persons so that they can recognize, understand and know how to tap into various sources of collective intelligence. Building a culture of collective intelligence-based knowledge intake, processing, integration and use is key to the success of using a vast amount of knowledge available in a systematic, beneficial manner for project work. This will be supported by CyberSEAS knowledge and achievement base.

(2) Assign a collective intelligence coordinator to the Cyber Stakeholder Community

Knowledge is important and brings clarity to thoughts and actions. Thus, it would be beneficial to assign a collective intelligence coordinator to projects (especially large-sized projects) to effectively use collective intelligence for project work. Assigning such a person provides focus to the efforts and helps to drive the use of available knowledge in a productive manner for project work. This coordination is provided by task Leader T8.1 in CyberSEAS project.

(3) Make collective intelligence as an input to EU level of Cyber-Physical protection of CIP and EPES *processes*

Systematic integration of collective intelligence into the EU process of protection EPES and CIP help in using the available knowledge reserves. Having collective intelligence as one of the inputs to exchanging processes helps experts and decision makers to think more clearly about tapping into the relevant sources of collective intelligence.

(4) Integrate key information in communication plans

Project organizations can improve their use of collective intelligence by adding information such as contact point names, social media identities, emails, phone numbers of sources (i.e. people or organizations) of collective intelligence in communication management plans. It will help project staff members to tap into the identified sources and bring available knowledge into the EPES Community.

(5) Build repositories to store and use the knowledge obtained from sources of collective intelligence inside and outside CyberSEAS environment

We developed collective intelligence repositories to store knowledge obtained from various knowledge sources. We understand that CyberSEAS project is just one of the numerous frameworks where we will create additional knowledge, best practices and new technological developments. Creating processes on how to use the knowledge obtained from collective intelligence helps to improve knowledge integration within the project organization system. Adding information about the experience of using collective intelligence in lessons-learned documents will help in the execution of future projects.

(6) Build leadership within the CyberSEAS Stakeholder Community

Organizations need to have leaders who possess vision, drive and adhere to use collective intelligence for work purposes. Therefore, offering discussion and training to target expert communities is critical to building a culture of using collective intelligence. This is important for the project and organizational work as well. The important role in this respect it has the operational coordinator who is also the task leader for T8.1 Stakeholder community building and clustering with other relevant projects and initiatives and CyberSEAS Stakeholder Community Coordination Board with all involved members.

It is important to understand that CyberSEAS Stakeholder Community is part of a broader network of EPES and broader CIP environment. This means that it was focused on integrated Cyber-Physical protection of EPES processes. This added value will transform towards to different EU institution environments with special focus such as EU DG ENER, REA, and Disaster Risk Management Knowledge Centre which is part of EU Joint Research Centre. This knowledge has been available also to other decision making and expert environments in EPES Critical Infrastructure Area.

2.3 Supporting interaction

The immediate social networks (online or offline) of CyberSEAS Stakeholder Community members are another key source of collective intelligence. It is not realistic to think that a project organization can be linked with all possible social networks to take benefit of knowledge available only within the networks.

Therefore, by tapping into knowledge and intelligence available within the immediate professional social networks of team-members, project organizations can expand their knowledge capacities and level of collective intelligence. Caution needs to be exercised to avoid legal complications or jeopardizing the project sensitive information when tapping into such networks though. This will be one of important the tasks of the Coordination Board to monitor with the support of SAB the content published from CyberSEAS project.

The availability of external experts outside project organization boundaries is one of the commonly known sources of collective intelligence for projects. Bringing in experts into CyberSEAS Stakeholder Community increases the collective intelligence of teams [4] as these experts transfer both tacit and explicit knowledge for the achievement of project objectives.

Project organization knowledge repositories consisting of lessons learned documents, past project information/documents, project management software-driven outputs, drawings, related documents, project management methodologies documents/templates, and information about new technologies are other sources of collective intelligence.

Experts working in partner target organization(s) can be a useful source of collective intelligence, as they can provide advice, documents and contact information of other experts when project organizations need any help. Knowledge repositories of client organization(s) consisting of organizational policies, standards, guidelines, templates and cultural context are also sources of collective intelligence for project work.

2.4 Exchange opportunities

Members of CyberSEAS Stakeholder Community provide knowledge through various communication channels in the form of (1) documents on best practice guidelines, standards, and certifications; (2) digital content on CyberSEAS website, blogs and social media; and (3) organizing conferences, symposiums, workshops and talks, (4) and also consortium members participating as invited speakers and panellists. These constitute another source of collective intelligence. Training offered by CyberSEAS bodies and other service providers helps the transfer of knowledge and expands *collective intelligence*.

Published scientific papers in research journals, conferences, and websites on issues related to CyberSEAS Stakeholder Community is also one of the key sources of collective intelligence. The industry-based reports, trends and future also add to collective intelligence. For this reason, it is very important to synchronize dissemination activities and dissemination channels (CyberSEAS web site, LinkedIn, Twitter and other channels) with Collective Intelligence activities within the framework of CyberSEAS Stakeholder Community.

2.5 Bottom up co-creation of practices

Proper functioning CyberSEAS Stakeholder Community Knowledge and intelligence Collecting process depend on a comprehensive approach related to directions of approaches for communication and exchanging new knowledge. We don't want to focus just on the classic top-down approach for sharing new knowledge and best practice from CyberSEAS project towards CyberSEAS Stakeholder Community members. The main efforts will be put into accelerating and supporting bottom-up co-creation of practice approaches [3]. This will provide collecting as wider as possible proposals on new innovation approach, best practices and new technology approaches. This will give us the opportunity to make a real comprehensive physical-cyber approach to EPES CIP and give an excellent base for further developments in policies, processes, technologies and human related activities for a higher level of CIP protection.

With a bottom-up approach, those who are more involved with the specifics of their field connected with EPES are included in the ideation and brainstorming process. These results are more harmonized and inclusive for the management system. Overall decision-making process has benefited from these frontline employees, practitioners and researchers who are engaged with their tasks at the "cutting edge" of the EPES. This feedback loop of information, suggestion and best practices is very important also in the lifetime of the project for adjustment and correction some additional steps in research processes.

The Benefits of Bottom-Up Approach Management

1. **All participants buy in:** One of the most obvious benefits from bottom-up approach is the fact that CyberSEAS Stakeholder Community participants felt far more involved with collective intelligence process and interested in its future success. They felt more involved to make processes and methodologies work out if they also feel ownership of their implementation. It also builds a consensus model which means that a practice is less likely to be introduced if the majority of the team doesn't agree with it.

2. **Risk identification:** As there is a greater degree of communication and feedback from those actively involved in CyberSEAS project tasks, there also was greater information about the level of risk contained in those tasks and how likely issues are to occur. This was also important for members outside of CyberSEAS environment.

3. **Broader knowledge base:** When you start using the bottom-up approach you could realize something which you should probably have already known, that individual members have far greater knowledge of their specific fields. This means that rather than giving imprecise instructions or underutilizing people's abilities, we can harness the full power of all members of CyberSEAS Stakeholder Community combined knowledge to make sure that Collective Intelligence process is running as effectively as possible.

4. **Improving collaboration:** The CyberSEAS Stakeholder Community could more likely be particular part or groups get siloed off and miss out on communicating with others involved in the project. This is a lot more likely to happen with the top-down approach, as there will be less opportunity for collaboration or hearing others' thoughts on the project's progress. The opposite occurs with bottom-up management, giving our expert community the best possible opportunity for collaborating and understanding the full breadth of CyberSEAS Stakeholder Community activities.

2.6 Sharing experience and knowledge

Today, the increased importance, complexity, interdependence and vulnerability of existing infrastructures require the creation of an effective Culture of Security for enhancing the protection of critical infrastructures (CIs). CyberSEAS aims to foster and support the creation of a Culture of Security for EPES. The realisation of such a vision can only be effective if the tools, knowledge and skills are available and if a knowledge sharing and collaboration Infrastructure is established as a common practice. In this perspective, the main step has been to create a wide EPES operator network and a Stakeholder Community on integrated cyber and physical protection of EPES where we would provide sharing experience and knowledge in different forms such as training schemes, operation procedures, knowledge, and recommendations for all stakeholders involved in EPES, including for policy making. The CyberSEAS webpage and other social media channels are intended as the main platforms to support CyberSEAS in fostering and supporting the creation of a Culture of Security and CIP for EPES. CyberSEAS Stakeholder Community creates and maintains relevant knowledge to improve the resilience and security of EU EPES, by:

- Classifying the EPES assets and systems and identifying/classifying their vulnerabilities;
- Analysing existing EPES cyber and physical threats and risks, and the corresponding scenarios;
- Assessing the state-of-the-art of cyber and physical detection technologies, in the context of EPES;
- Identifying EPES-specific criteria to assess the cyber and physical risk and forecast emerging and future threats, while analysing cascading/interconnection effects;
- Improving EPES risk management ability, promoting a stronger stress-test-based risk and resilience assessment culture and effective risk-related information sharing among all

stakeholders, viewing risk assessment in an interconnected and interdependent perspective.

Relevant information on threats, vulnerabilities and risks for EPES and information sharing methods and tools proposed by CyberSEAS have been available through the Stakeholder Community network. Behind the design and development of the CyberSEAS Stakeholder Community network is the need to upgrade the capability to address the continued increase of threats in the EPES security domain, affecting information technology, physical environment, people and how these have become crucial. The design and implementation of the material blend cyber and physical aspects and the creation of study material, best-practices factsheets, guidelines, related to the cyber-physical protection of EPES would be available throughout the platform. This would also provide base for supporting interactions, exchange different opinions, top-down and bottom-up co-creation of practices, sharing of experience and knowledge. This community offers an online social network which includes content and information sharing, search and retrieval, community building (using current online 'social' paradigms), online discussions and idea sharing, work management tools (e.g. calendar), and people management and network building (e.g. user profiles, people search, user-groups, etc.). Such approach would enable CyberSEAS to create a distributed (i.e. multi-country) stakeholder community. CyberSEAS Stakeholder Community represents a useful community-based tool simplifying exchange of information among all the stakeholders involved. The community provides a Collaborative Environment with a set of collaborative services that allow to share, transfer knowledge, and promoting collaboration. The CyberSEAS Stakeholder Community aims to be the enabler (and at the same time supportive) framework for the development of a collaborative environment characterised by the presence of many stakeholders who actively collaborate. The adoption of social collaboration models is based on the development of collective intelligence, transparency and the concept of communities. This approach aims at integrating explicit knowledge (that is, directly represented by users in a structured way) with the implicit one the one inserted by them in typically unstructured content (blogs, wikis, communities, etc.) and to the contextual extraction, derivation, determination of new knowledge. Existing knowledge (e.g. best practice, guidelines, lessons learnt, procedures, etc.) related to the cyber-physical protection of EPES can help in making the decisions and new knowledge can be shared by the stakeholders. As a result, tools and services to support and stimulate the usage, sharing and creation of knowledge to promote collaboration, coordination and to improve and support collaborative decision making have been implemented.

3 Cross-dissemination activities and organizational structures (UPDATED)

As described in chapter [2.2. Methodology and procedures for the process of creating a Stakeholder community]. The main lines of activities in the project concern:

1. CyberSEAS Project Partners;
2. Advisory Board members;
3. CyberSEAS MIG (Market Interest Group)
4. Related Projects and Initiatives;
5. Community target organizations, standardizations and legislative bodies.

Public outreach and community building is important for better shaping approaches methods toward different target environments. This should be also taken in account in relation to the creation of the CyberSEAS Stakeholder Community target groups and messages.

This activity is foreseen in the creation of CyberSEAS Stakeholder Community, and it involves the following classes of stakeholders with the following main messages:

1. EPES operators (such as the end user of EPES infrastructure (TSOs, DSOs, DER owners, etc.) and industrial companies (such as the manufacturer and/or supplier of products and services to end users)
   Message: enhancing cyber security resilience as it sends a governance, strategic and internal management positive message, setting new best practices
2. Security and ICT industry
   Message: highlight users' need scope and proposed technical solutions
3. Standardization bodies
   Message: show standardisation advantages of resilience management
4. Academy
   Message: high scientific stakes
5. Policy makers
   Message: contribute to setting EU wide regulations for enhancing EPES global security
6. Public authorities managing EPES related security
   Message: enhance cooperation with EPES for crisis management and global security
7. First responders
   Message: enhance cooperation with EPES for security
8. Citizens
   Message: resilience cyber security management will make your community safer, get involved to know appropriate behaviours

9. Civil Society at large
   Message: resilience management makes life near safer.

We put special focus in providing detail SOTA on two target environment environments (pillars) of CyberSEAS Stakeholder Community. These pillars are: (1) Related Projects and Initiatives and (2) Community target organizations, standardizations and legislative bodies.

3.1 SOTA analyses for Setting up and consolidating a network between relevant EU initiatives, relevant H2020 projects and other expert Community

In order to properly understand the possible EU initiatives, the relevant H2020 projects and the other professional community, it is necessary to carry out a detailed situational analysis (SOTA). We have analysed a very wide range of possible target environments, which could later represent a good opportunity to integrate the CyberSEAS project and strengthen the whole set of activities within the framework of EPES.

We focused analysis on two major network environments:

(1) Related Projects and Initiatives and

(2) Community target organizations, standardizations and legislative bodies.

3.1.1 Related projects and Initiatives

The European Commission has acknowledged the need for a specific approach to the cybersecurity of the energy sector through the 2019 recommendation [5]. The same recommendation has been pushing stakeholders such as ENTSO-E to work on Network Code specifically tailored to manage cyber-security on smart grids.

Moreover, the Electricity Risk Preparedness Regulation [6] has acknowledged the demand for an electricity domain-specific common and cooperative framework to assess risks to the security of electricity supply, including cyber-risks, while envisioning common rules for managing crisis situations. Relevant on-going initiatives and working groups could be interesting for CyberSEAS project collaboration.

Energy Initiatives

a. **European Network of Transmission System Operators for Electricity (ENTSO-E)** (https://www.entsoe.eu/)

ENTSO-E, the European Network of Transmission System Operators for Electricity, is the association for the cooperation of the European transmission system operators (TSOs). The 39 member TSOs representing 35 countries are responsible for the secure and coordinated operation of Europe's electricity system, the largest interconnected electrical grid in the world. In addition to its core, historical role in technical cooperation, ENTSO-E is also the common voice of TSOs. (especially through the following partners: ELES, HOPS, TEL)

b. **CIGRE** (https://www.cigre.org/)

Established in 1921 in Paris, France, CIGRE is a global community committed to the collaborative development and sharing of power system expertise. The community features thousands of professionals from over 90 countries and 1250 member organizations, including some of the world's leading experts. At its heart are CIGRE's 59 in country National Committees offering diverse technical perspectives and expertise from every corner of the globe.

CIGRE operates the world's foremost knowledge program, spanning 16 domains of work encompassing all the core areas of the power system. Across these domains, 250+ Working Groups draw and build on practical expertise to solve existing and future challenges facing the power system.

c. **Data Management WG of the BRIDGE Cluster** (https://bridge-smart-grid-storage-systems-digital-projects.ec.europa.eu/working-groups/data-management)

The Data Management WG within the BRIDGE Cluster of Smart Energy grid projects, managed by EC DG Energy), delivered a report on Cybersecurity and Resiliency to identify and assess, among other things, how and to what extent on-going H2020 Smart Energy grid projects are able to implement the provisions set in the above Recommendation [7]. CyberSEAS connects to both working groups and projects of the BRIDGE cluster - including the Data Management Working Group and its involved projects ELSA, Integrid, Osmose and WiseGrid (partner: ENG), FutureFlow, Migrate, Osmose (partner: Eles), Interflex (partner: RWTH), Sensible (Empower). (through projects: PLATOON (ENG), WiseGrid (ENG), Osmose (ELES), Interflex (RWTH) and Sensible (ENERIM)

d. **ETIP-SNET Smart grid Technology Platform WG4 on Energy Digitization** (https://smart-networks-energy-transition.ec.europa.eu/working-groups/wg4)

The ETIP-SNET Smart grid Technology Platform WG4 on Energy Digitization [8]considers cybersecurity as one of the potential research areas for the energy sector in the coming years. (Direct connections implemented through partners ELES, ENG, IKL, RWTH and ZIV).

e. Critical Energy Infrastructure Security Stakeholders Group (CEIS-SG)

The Critical Energy Infrastructure Security Stakeholders Group (CEIS-SG), a think-tank and information exchange forum to guide and coordinate efforts to improve the security and resilience of critical energy infrastructure (CEI), supported by the EU project DEFENDER project (coordinated by partner ENG);

f. Smart Grid Task Force Expert Group 2

(https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=2892)

The Smart Grid Task Force [CSEA15] provides regulatory recommendations for privacy, data protection and cybersecurity in the smart grid environment within Expert group 2 - including the template for Data Protection Impact Assessment for Smart Grid and Smart Metering systems [9].

Cybersecurity Initiatives

a. The European Union Agency for Cybersecurity (ENISA) (https://www.enisa.europa.eu/)

The European Union Agency for Cybersecurity (ENISA) contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union in cooperation with the wider community.

(Luigi Romano (Tech. Coord.) appointed as expert for the ENISA Research and Innovation Annual Report; SI-CERT (Slovenian CERT) active collaboration with ENISA).

b. European Network for Cyber Security (ENCS) https://encs.eu/

ENCS stands for European Network for Cyber security (ENCS). They are a non-profit organization owned by grid operators (DSOs and TSOs) that want to improve cyber security in the EU. (Through members: ELES, HOPS)

c. MeliCERTes network

The MeliCERTes network of collaboration for CSIRTs at the European level is a major initiative, supported by the CEF, to streamline cross-border collaborations and faster reaction time for new cyber-attacks. This is a key asset and CyberSEAS aims to connect its governance and communication processes to the MeliCERTes platform - this is tested in a dedicated scenario and is supported through the Slovenian CERT and Polish NASK (refer to letter of subcontracting to partner GT).

d. European Cybersecurity Organization (ECSO) (https://ecs-org.eu/)

ECSO among others defines the R&I roadmap in cyber security to strengthen the EU eco-system by understanding and coordinating the challenges towards digitalization of the industrial sectors and developing a coherent strategy with other cPPP and EU initiatives.

The mission of Working Group 6 is to contribute to defining the cyber security EU R&I roadmap and vision to strengthen and build a resilient EU ecosystem. From the analysis of the challenges of digitalization of the society and industrial sectors, this WG identifies what are the capacities and capabilities to sustain EU digital autonomy by developing and fostering trusted technologies. (Through ECSO members: ACS, ENG, GT and WINGS)

e. Participation in the Women4Cyber initiative (https://women4cyber.eu/)

Women4Cyber is a non-profit European private foundation with the objective to promote, encourage and support the participation of women in the field of cybersecurity.

f. European Competence Network of Cybersecurity Centres (ECCC) (https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre)

With the setting up of the European Competence Network of Cybersecurity Centers of Excellence Europe pools its cybersecurity expertise to implement a common vision of a more secure digital Europe. Across the 4 centers, industry and academia are working together to innovate and pilot these innovations across all domains. CyberSEAS will tap on the resources of the networks when creating the complete portfolio of solutions, to feed its governance mechanisms, interact on certification and training approaches and review its methodological measures.

CyberSEAS benefits from direct connections to the following centers of excellence:

- CONCORDIA - (ACS).
- CyberSec4Europe – (ENG, TLX) .
- ECHO – (GT, SMV).
- SPARTA – (CINI, Fraunhofer (and NASK as supporting subcontractor organization).

g. European Energy Sharing & Analysis centre (EE-ISAC) (https://www.ee-isac.eu/)

The EE-ISAC is an industry-driven, information sharing network of trust. Private utilities, solution providers and (semi) public institutions such as academia, governmental and non-profit organizations share valuable information on cyber security & cyber resilience.

EE-ISAC aims to improve the resilience and security of the European energy infrastructure, by sharing trust-based information and enabling a joint effort for the analysis of threats, vulnerabilities, incidents, solutions, and opportunities. EE-ISAC offers a community of communities to facilitate this proactive information sharing and analysis, allowing its members to take their own effective measures.

EE-ISAC [10] to push EPES stakeholders to increase the level of cooperation and accordingly share data and best practices on cyber-attacks in a static way -reports used in CyberSEAS include the ‘Cyber Security Incident Response white paper [11].

For the future cooperation with CyberSEAS we should especially find interesting the following working groups:

- Threat Intelligence & Incident Analysis-Response
- Malware Information Sharing

CyberSEAS' relationship withData initiatives

a. International Data Spaces Association (IDSA) (https://internationaldataspaces.org/)

Especially through Energy Data Access Alliance the European Commission's 2020 Strategy for Data [12] foresees the creation of sector-specific Common Data Spaces, and the publication of the governance in relation to these spaces by end of 2020. This governance is of direct relevance to CyberSEAS, as well as the work of the International Data Spaces Association [13] (IDSA), with a membership of 101 organizations from 20 countries, which aims to guarantee data sovereignty by an open, vendor-independent architecture for a peer-to-peer network which provides usage control of data from all domains. In this data exchange domain, the DSOs from Denmark, Estonia, Finland, France, Lithuania, the Netherlands Poland joined forced in November 2019 with the creation of the Energy Data Access Alliance [14] - an effort led by Estonia's TSO, Elering.

b. Gaia-X Foundation

(https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html)

With Gaia-X, representatives from business, science and politics on an international level create a proposal for the next generation of data infrastructure: an open, transparent and secure digital ecosystem, where data and services can be made available, collated and shared in an environment of trust.

We see CyberSEAS cooperation especially in relation of use cases of the Energy ecosystem working group:

- Infrastructure data for new business models
- Edge data centers

- Aggregator Services for Energy Communities

Involvement in the Gaia-X Foundation as part of the workstreams on technical implementation and user ecosystems and requirements, which includes an Energy ecosystem working group. Gaia-X aims towards a trusted European data infrastructure with a strong focus on data security and sovereignty.

CyberSEAS w.r.t. Critical Infrastructure Protection

a. European Cluster for Securing Critical Infrastructure (ECSCI) (https://www.finsec-project.eu/ecsci)

The main objective of the ECSCI cluster is to create synergies and foster emerging disruptive solutions to security issues via cross-projects collaboration and innovation. Research activities focus on how to protect critical infrastructures and services, highlighting the different approaches between the clustered projects and establishing tight and productive connections with closely related and complementary H2020 projects. To promote the activities of the cluster, ECSCI organizing international conferences, and national or international workshops, involving both policy makers, industry and academic, practitioners, and representatives from the European Commission.

The following projects are included in ECSCI:

H2020 DEFENDER – critical Energy infrastructure Protection

H2020 NASTACIA - Advanced Networked Agents for Security and Trust Assessment in CPS / IOT Architectures

H2020 CYBERSANE - Dynamic countering of cyber-attacks

H2020 FINSEC - Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures

H2020 ENSURENSEC - Safeguarding the Digital Single Market's E-Commerce Ecosystem

H2020 INFRASTRESS - Improving resilience of sensitive industrial plants & infrastructures exposed to cyber-physical threats, by means of an open testbed stress-testing system

H2020 ENERGYSHIELD - Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures

H2020 FEATURECLOUD - Federated, Secure and Private AI for Everyone

H2020 SAFECARE – Integrated cyber-physical security for health services

H2020 SOTER – Cyber security optimization and training for enhanced resilience in finance

H2020 PHOENIX – Electrical Power systems shield's against complex incidents and extensive cyber and privacy attacks

H2020 IMPETUS - Intelligent Management of Processes, Ethics and Technology for Urban Safety

H2020 SMARTRESILIENCE – Smart Resilience project

H2020 7SHIELDS – Advanced technologies against cyber&physical threats for space ground segments

H2020 SATIE - Security of Air Transport Infrastructure of Europe

H2020 STOP-IT - Secure and protect your water infrastructures

H2020 RESISTO - Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe

H2020 SEALED GRID - Scalable, trusted, and interoperable platform for secured smart grid

H2020 SECURE GAS - Securing The European Gas Network

H2020 SPHINX - A Universal Cyber Security Toolkit for Health-Care Industry

H2020 SAFTY4RAILS – Safety for Rails

H2020 PRECINCT - Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber-physical Threats and effects with focus on district or regional protection

H2020 EU-HYBRID – Pan European Network to counter Hybrid threats

H2020 PRAETORIAN - Protection of Critical Infrastructures from advanced combined cyber and physical threats

H2020 CyberSEAS – Cybersecurity in the Electrical Power and Energy System

CyberSEAS project will organize cooperation and collaboration in ECSCI cluster activities but on the other hand will search direct connections with individual H2020 project involved in ECSCI.

b. CyberEPES Cluster

This cluster of projects is focused on projects related to Energy grids and Cyber security.

Key issues for this cluster are:

1. Coordination of activities/exploring commonalities-difference of approaches related to risk identification /assessment.

2. Coordination of activities/ Exploring commonalities-difference of approaches related to SOC/ SIEM tools.

3. Coordination of activities/ Exploring commonalities-difference of approaches related to legacy components (e.g. SCADA/ RTU) hardening and/ or middleware components (e.g. universal gateways, honeypots, "ghost" RTUs, etc).

4. Coordination of activities/ Exploring commonalities-difference of approaches related to threat isolation

5. Organization of common trials among research initiatives

6. Coordination of interaction with BRIDGE groups (on architecture, business models, etc.)

7. Coordination of interaction with CIRTS/ CERTS etc.

8. Coordination of contributions related to NIS/ Cybersecurity Act (e.g. certification https://www.enisa.europa.eu/topics/nis-directive

9. Create a Culture of Knowledge and Security, as a horizontal action to support the upskilling of current human resources and the development of appropriate skills and competence in the next generation of cyber security professionals.

H2020 ELECTRON – Resilient and self-healed Electrical power nanogrid

H2020 ENERGYSHIELD - Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures

H2020 PHOENIX – Electrical Power systems shield's against complex incidents and extensive cyber and privacy attacks

H2020 SDN-microSENSE – SDN microgrid resilient electrical energy system

H2020 CyberSEAS -
Cybersecurity in the Electrical Power and Energy System

c. Community of Users

The activities related to the Community of Users (CoU) (https://www.securityresearch-cou.eu/challenge) concern involving CyberSEAS project into the mainstream of the CoU, looking at the CoU main challenges as related to SIPS.

This means, that EPES play a significant role in a world where the risks of man-made and natural disasters are ever-growing the key question is how societies can enhance their resilience and become better prepared. Current threats, ranging from cyber environment, natural disasters to crime and terrorism, are posing challenges to the security of citizens, infrastructure and the environment. Strengthening EPES capacities in disaster risk and crisis management and increasing resilience form the backbone of key EU policy and research challenges.

The security landscape for EPES is complex. It covers many different sectors, numerous communities and a vast range of operational procedures for preparedness, prevention, detection, surveillance, response, and recovery. Therefore, effective coordination and interaction are essential between the various stakeholders involved. These activities should also produce innovative research outcomes in terms of technologies, training and network building in the area of EPES. Through the engagement of CyberSEAS project the Community of Users will be able to address better the issues related to EPES by making the latest policy updates and research outputs, accessible and more visible in the CoU events, CoU webpage and the CoU annual mapping document.

The issues related to the critical infrastructures (CI) will be dealt with in the Cluster of CI projects (ECSCI), where CyberSEAS is a member and participates in its activities.

3.1.2 Community target organizations, standardizations and legislative bodies

Of course, the strong synergy of the CyberSEAS project with other organizations must be sought in the wider social environment. Particularly important in this context are also the individual national professional associations, standardization organizations and government bodies, which bring together important stakeholders who are directly or indirectly related to ensuring the safe and continuous operation of EPES. For this reason, we will look for the widest possible range of stakeholders as part of the monitoring and search for possible connections. We will take some environments as test ones due to their appropriate controllability so that we can see the possibilities for wider cooperation in the larger national environments on their example. Such an example will be cooperation with the Slovenian Association for Corporate Security.

a. Network of CSIRTS

The Network and Information Systems (NIS) Directive [15] has set provisions for the designation of national competent authorities and the creation of general domain-agnostic computer-security incident response teams (CSIRT) - which forms a basis for the energy-domain specific collaboration mechanisms enhanced through CyberSEAS. Additional authorities and roles have been based in Directive on measures for a high common level of cybersecurity across the Union (NIS-2) [16].

b. CEN https://www.cencenelec.eu/about-cen/

The European Committee for Standardization is one of three European Standardization Organizations (together with CENELEC and ETSI) that have been officially recognized by the European Union and by the European Free Trade Association (EFTA) as being responsible for developing and defining voluntary standards at European level.

c. CENLEC https://www.cencenelec.eu/about-cenelec/

The European Electrotechnical Committee for Standardization is one of three European Standardization Organizations (together with CEN and ETSI) that have been officially recognized by the European Union and by the European Free Trade Association (EFTA) as being responsible for developing and defining voluntary standards at European level.

d. National associations

National association are important professional target environments. We present the Slovenian example in the perspective of possible work also with the other national associations.

Slovenian Corporate Security Association which is also part of SE Europe Corporate Security association associates with almost all-important organizations related to EPES. Besides the direct EPES organizations such as TSO, DSO's, producers of electricity, retailers also the important government and energy supervisory organizations take part in the Slovenian Corporate Security Association such as the Ministry Republic Slovenian for Infrastructure, Ministry Republic Slovenian for Justice, Electricity distribution system operator (SODO) and others. Beside these also all-important actors related to cyber security are included such as the Government Security information office Republic of Slovenia, SI-CERT, Communications Networks and Services Agency of the Republic of Slovenia (AKOS). This will give us an opportunity to evaluate and test cooperation and implementation possibilities between CyberSEAS project and this related expert network. After that, findings could be a good example for setting cooperation possibilities with similar national networks in bigger countries.

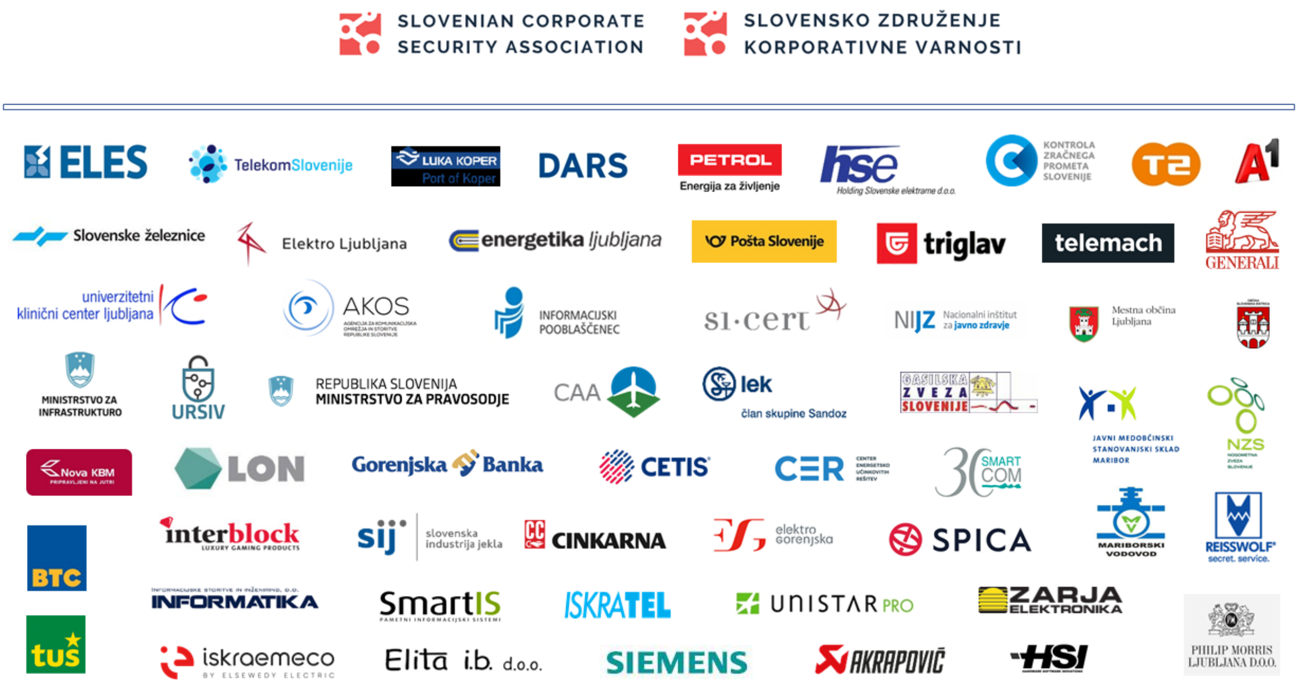

SLOVENIAN CORPORATE SECURITY ASSOCIATION
SLOVENSKO ZDRUŽENJE KORPORATIVNE VARNOSTI
ELES
TelekomSlovenije
LUKA KOPER Port of Koper
DARS
PETROL Energija za življenje
hse
KONTROLA ZRAČNEGA PROMETA SLOVENIJE
T2
A1
Slovenske železnice
Elektro Ljubljana
energetika ljubljana
Pošta Slovenije
triglav
telemach
GENERALI
univerzitetni klinični center ljubljana
AKOS
INFORMACIJSKI POOBLAŠČENEC
SI-CERT
NIJZ Nacionalni inštitut za javno zdravje
Mestna občina Ljubljana
MINISTRSTVO ZA INFRASTRUKTURO
URSIV
REPUBLIKA SLOVENIJA MINISTRSTVO ZA PRAVOSODJE
CAA
lek član skupine Sandoz
GASILSKA ZVEZA SLOVENIJE
JAVNI MEDOBČINSKI STANOVANJSKI SKLAD MARIBOR
NZS
Nova KBM
LON
Gorenjska Banka
CETIS
CER
30 SMART COM
MARIBORSKI VODOVOD
REISSWOLF secret. service.
BTC
interblock
sij slovenska industrija jekla
CINKARNA
elektro gorenjska
SPICA
INFORMATIKA
SmartIS
ISKRATEL
UNISTAR PRO
ZARJA ELEKTRONIKA
PHILIP MORRIS LJUBLJANA D.O.O.
tuš
iskraemeco
Elita i.b. d.o.o.
SIEMENS
AKRAPOVIĆ
HSI

Figure 4: Members of Slovenian Corporate Security Association

(Source: https://www.ics-institut.si/en/slovensko-zdru%C5%BEenje-korporativne-varnosti)

We could also invite and cooperate with other partner associations. For example, we could indicate regional associations such as SE Europe Corporate Security Associations. These associations besides Slovenian Corporate Security Association are Croatian security management association, Association for corporate security from N. Macedonia and Serbian Corporate Security Association.

SEECSA
SE Europe Corporate Security Association
SLOVENSKO ZDRUŽENJE KORPORATIVNE VARNOSTI
Hrvatska Udruga Menadžera Sigurnosti
САМКБ Српска Асоцијација Менаџера Корпоративне Безбедности
ASSOCIATION FOR CORPORATE SECURITY
ASOCIJACIJA MENADŽERA BEZBJEDNOSTI CRNE GORE

Figure 5: Members of South-East Europe Corporate Security Association

4 Road map for Creation Stakeholder Community

This list of relevant initiatives and activities have been further monitored and enhanced during the project; the key strategy for CyberSEAS is to ensure that it maintains operational links to these activities to build on information and efforts when these exist and to contribute the results of CyberSEAS, such as the extended governance and the experiences acquired through the piloting of cyber-secure interactions between operators, including the extension towards consumers and connected retailers. Another important dimension is that in addition to this very active context for cybersecurity in the energy sector, EPES stakeholders and in particular power network operators, have, in many cases, developed or adopted cyber-risk assessment models and appropriate technology components (such as SIEMs) which they leverage to predict and detect potential cyber-threats that may undermine their respective business processes. CyberSEAS complements this work by extending the collaboration to the complete supply chain.

The road map for creating Stakeholder Community has been divided into six periods. Each task has been respected with the most important activities for the period. The timeline for the contribution to expanding CyberSEAS Stakeholder Community activities is presented in figure 5. The contribution to the creation of CyberSEAS Stakeholder Community plan, as presented, has to match the reality of resources available in CyberSEAS project, both in terms of person months as well the lifespan of the project.

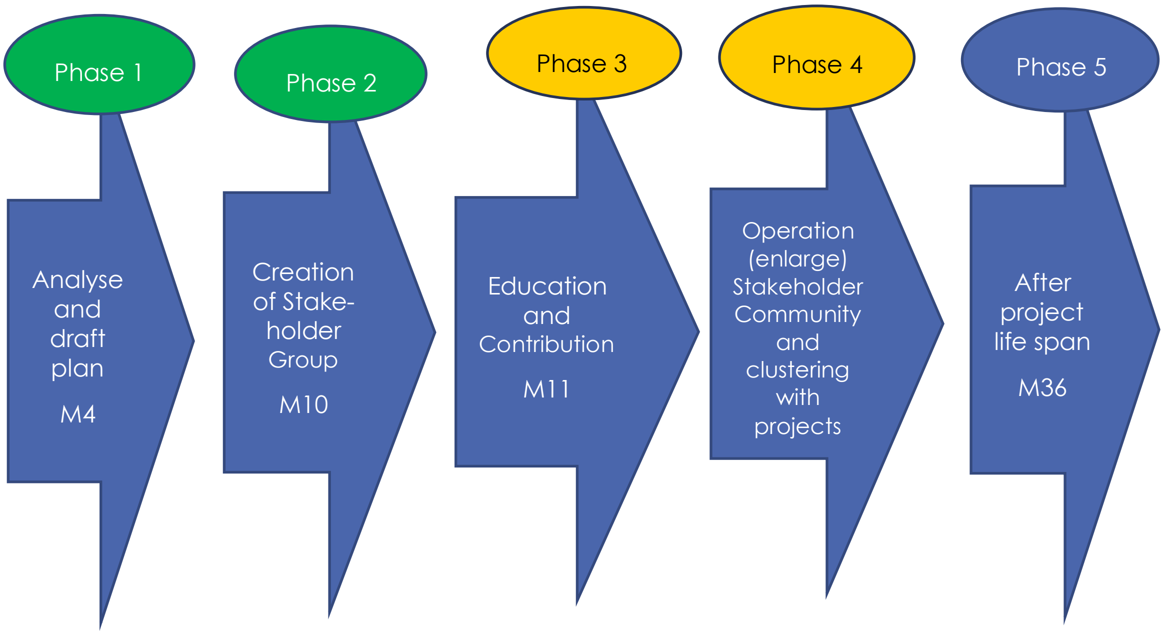

Phase 1
Analyse and draft plan
M4
Phase 2
Creation of Stake-holder Group
M10
Phase 3
Education and Contribution
M11
Phase 4
Operation (enlarge) Stakeholder Community and clustering with projects
Phase 5
After project life span
M36

Figure 6: Contribution to Stakeholder Community timeline

The first and second phases have been dedicated to analysing existing possibilities in the creation of CyberSEAS Stakeholder Community. This period was also important for preparing a Draft plan of creation CyberSEAS Stakeholder Community. The second period corresponded to Stakeholder Community framework setting and its operationalization.

The next period was strongly connected with the previous one and has been focusing on detail education and training for familiarization with CyberSEAS Stakeholder Community and possible communication channels for contributing new knowledge to the system and receiving best practices from the project developing processes. It is followed by a period when the full operation of CyberSEAS Stakeholder Community was started, and special attention was put on the extension of the community. As is the case already in the draft period, the evaluation period involved even more contacts with the target expert persons and organizations and related communication efforts. The results of all phases of these processes have been summarised in chapter of D5.2 . Results and outcomes of clustering with relevant projects and initiatives. The important indication of best practice was providing the synergies between the Stakeholder Community and CyberSEAS MIG. This have been manifested since the beginning of the project implementation, from the "construction" phase, and later through the stakeholder engagement activities, with a special emphasis on the market-related aspects, through the effective collaboration with Market Interest Group, mostly within Phases 3 and 4.

Operationally wise the fourth period had prevailed by the two-direction contribution to CyberSEAS Stakeholder Community and enlargement the number of participants. The amount of contribution was highly dependent on the interest in quality information among individual stakeholders in the Stakeholder Community and of course from interest of target EPES organizations in national and international level. In phase 4 we organized different workshops for Stakeholder Community users with a special focus to exchange relevant information. This was an important base for successful usage of the Stakeholder Community framework for exchanging best practices, new knowledge, and the latest technical developments in EPES area. Special attention in this phase of evolution of creation CyberSEAS Stakeholder Community was focus on core membership which is already part of this community. In this phase also contribution started to be a main part of processes. The most important planed target groups you can find also in chapter 3 of this report.

It must be also noted that the research in the project have been pre-competitive, and the expected results of the project have been prototypes, not commercial products. The most important public deliverables which provided best practices, lessons learned, and new operational approaches were released at M30-M36. All these reasons showed us that phase 5 had crucial role in how to transfer new knowledge in the period after the life cycle of CyberSEAS project.

5 Results and outcomes of Stakeholder community building and clustering with relevant projects and initiatives (NEW)

In this important chapter, we conducted a comprehensive review of the activities carried out and the results achieved during the CyberSEAS project in the area of stakeholder community building and clustering with relevant projects and initiatives. Through this thorough overview, we will also highlight the lessons learned that we have identified through the activities undertaken in community building, the exchange of significant best practices and experiences, and the collection of feedback, which has been crucial for aligning subsequent steps throughout the project. Our primary aim was to achieve effective goals that were closely aligned with the needs and challenges of the real environment within the EPES.

To begin with, we will detail the various strategies employed to engage stakeholders and build a robust community around the CyberSEAS project. This includes identifying key stakeholders across different sectors, establishing communication channels, and organizing events such as workshops, webinars, and conferences that facilitated knowledge sharing and collaboration. The creation of these networks was essential not only for the dissemination of project results but also for fostering partnerships that could extend beyond the project's lifespan.

We will also examine the clustering efforts with relevant projects and initiatives. This involved mapping out existing projects with similar or complementary objectives and establishing formal and informal partnerships. By clustering with these projects, CyberSEAS benefited from shared resources, expertise, and wider dissemination channels. These partnerships often led to joint activities, such as co-hosted events and collaborative research efforts, which enhanced the overall impact of the project.

Furthermore, we will delve into the specific tools and platforms used to facilitate community building and clustering. Online platforms played a critical role in maintaining engagement and communication among stakeholders.

An essential component of our review will be the feedback mechanisms that were put in place. Regular surveys, feedback forms, and direct consultations were conducted to gather input from stakeholders. This feedback was invaluable in understanding the evolving needs and challenges faced by the EPES community, allowing the project to adapt its strategies and activities accordingly. For example, adjustments were made to the content and focus of workshops based on participant feedback, ensuring that the sessions remained relevant and useful.

We also discussed the lessons learned from these activities. One key lesson was the importance of flexibility and adaptability in community building efforts. The dynamic nature of the EPES sector meant that priorities and challenges could shift rapidly, requiring a responsive approach. Another important lesson was the value of trust-building among stakeholders. Developing a strong sense of trust and collaboration was fundamental to the success of the project, as it encouraged open communication.

In conclusion, this chapter provided a detailed account of the CyberSEAS project's efforts in stakeholder community building and clustering. By examining the strategies, tools, feedback mechanisms, and lessons learned, we aim to offer insights that can guide future activities in EPES cyber security domain. The activities carried out not only contributed to the immediate success of the CyberSEAS project but also laid the groundwork for ongoing collaboration and innovation within the EPES community.

5.1 Results and outcomes of Stakeholder Community building

In the CyberSEAS Stakeholder Community, a total of 101 experts had joined by the end of the project's operational cycle. Six major project meetings were organized for this community. Members were kept informed about project developments, best practices, and other significant information through various communication channels throughout the project's duration. They were also given the opportunity to participate in all other events organized or co-organized by the CyberSEAS project. On all community meeting were invited also all Advisary Board members.

A key aspect of the community was the emphasis on two-way communication. The seven main meetings of the CyberSEAS Stakeholder Community provided an excellent opportunity for members to share their experiences, perspectives, recommendations, and suggestions for improving individual activities, thereby aligning the project's development with the real needs of the EPES sector.

To further enhance the effectiveness of stakeholder engagement, the project team utilized a variety of digital platforms and tools. These included webinars, online forums, and collaborative workspaces, which allowed stakeholders to interact seamlessly regardless of geographical constraints.

Significant attention was also given to gender balance when expanding the EPES Stakeholder Community. Besides involving female experts in the field of cybersecurity, efforts were made to include discussions and presentations on activities of initiatives such as Women in Cyber and similar programs. This inclusive approach not only enriched the community with diverse perspectives but also promoted a culture of equality and representation within the field.

In forming and expanding the community, the focus was not solely on cybersecurity. The aim was to include experts from related professional fields, particularly those from organizations involved in critical infrastructure. This holistic approach ensured a diverse and comprehensive stakeholder community capable of addressing a wide range of issues relevant to the EPES sector. Experts from fields such as energy management, environmental sustainability, risk assessment, and emergency response were actively sought out and included in the community. This multidisciplinary integration facilitated a more robust and well-rounded discussion on the challenges and solutions pertaining to critical infrastructure protection.

Moreover, the community's engagement went beyond mere participation in meetings and events. Stakeholders were encouraged to contribute to the development of project deliverables, such as white papers, technical guidelines, and policy recommendations. Their insights and feedback were invaluable in refining the project's outputs to ensure they were practical, applicable, and impactful.

The CyberSEAS project successfully built a vibrant and interactive stakeholder community, facilitating valuable exchanges and ensuring the project's alignment with industry needs and trends. The community's contributions significantly enhanced the project's outcomes, demonstrating the importance of inclusive and engaged stakeholder involvement in complex projects like CyberSEAS. The lessons learned from this community-building effort highlight the critical role of stakeholder collaboration in driving innovation, fostering resilience, and achieving sustainable development in the EPES sector.

Let's take a detailed look at the data regarding which sectors were represented within the CyberSEAS Stakeholder Community.

Sector	**Number of members**
Energy domain	32
Critical infrastructure	16
International associations	5
National Associations	2
Governmental institutions	5
R&D area	19
Education institutions	3
Business organization	9

Clusters and related projects	7
Local communities	3
Total:	**101**

Table 2: Representation on sectors in CyberSEAS Community

In the following, we aim to present the specific activities conducted during the six main meetings of the CyberSEAS Stakeholder Community members and the important feedback we received from them through various forms of communication.

The First meeting was organized on 29. NOV 2022

Time	**Presentation**	**Presenter**	
10:00-10.05	Welcome and introduction	Denis Caleta (ICS)	
10:05-10:45	Presentation results and evolution of project CyberSEAS in the first year	Paolo Roccetti (ENG) – project coordinator	
10:45-11:15	Open discussion about possible suggestion regarding the evolution of project course	All community members	
11:15-11:45	Open discussion about next steps and possible activities in CyberSEAS Stakeholder Group	All community members	
11:50	Conclusion of the meeting	Denis Caleta (ICS)	

Table 3: Program of 1st Stakeholder Community meeting

The main conclusion from the first meeting:

Main conclusion points:

- We had round table introduction of all members of CyberSEAS community present on the first meeting;
- After CyberSEAS project presentation we had interesting discussion and questions related to approaches for pilot testing, where is testing focus in infrastructure or data’s, about framework of threat agents used in project;

- We agreed that we could have meetings of CyberSEAS Stakeholder Community in 3-5 months period;
- Each partner of Stakeholder Community searched about the possibility to invite some additional members from his/her network. Stakeholder community coordinator (Denis Caleta) provided information and invitation letter for purpose of inviting new members. All new members indicate their intention to joining the community through the link https://cyberseas.eu/contacts/.
- The possible collaboration from different projects and possible cooperation in Cybersecurity Innovation Cluster for EPES https://cyberseas.eu/cyberepes/ is also more than welcome.
- All members got short survey to indicate their expectations and proposals for further work of the CyberSEAS Community;
- CyberSEAS project presentation was sent to all CyberSEAS Stakeholder Community members.

The second meeting was organized on May 29, 2023

Time	Presentation	Presenter	
11:00-11.10	Welcome and introduction	Dr. Denis Caleta	
11:10-11:30	Main steps in evolution of CyberSEAS project and preparation to mid review	Dr. Paolo Roccetti (ENG)	
11:30-11:50	WP3/WP7 - usage of attack trees to model cyber threats to energy infrastructures (summarizes the work done in T3.1 for the Attack trees of each pilot)	Dr. Giovanni Mazzeo (CINI)	
11:50-12:10	Decision-making process for the selection of mitigations against cyberattacks	Dr. Andrej Bregar (INF)	
12:10-12:30	The challenge of Legacy. Elements of critical infrastructure, including the cybernetics, have very long lifetimes, especially compared to the pace of creation and mitigation of cybersecurity vulnerabilities in cloud ICT. What is the impact on managed migration and upgrades	Dr. Frank Amand (WP7)	

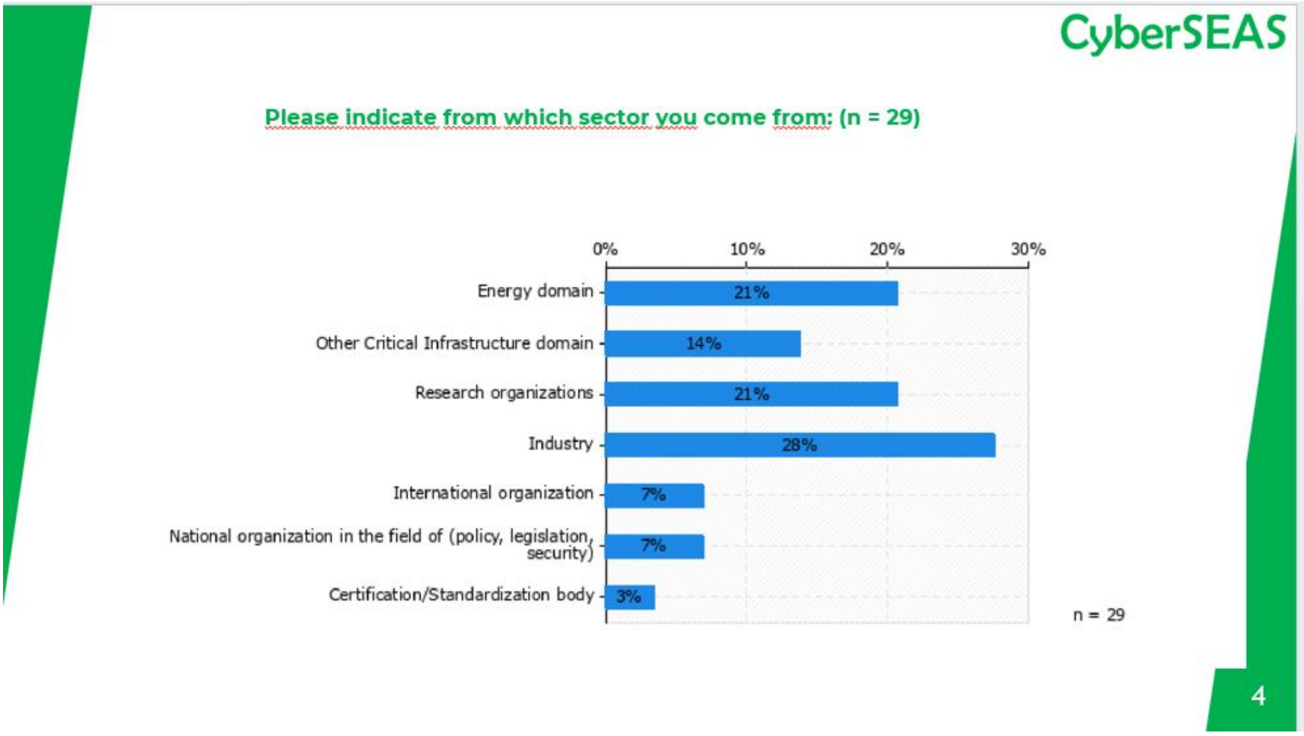
12:30-12:40	Results with short analyses of survey made among CyberSEAS Stakeholder Community members and future steps	Dr. Denis Caleta (ICS)	
12:40-13:30	Discussion and proposals for the next meeting	All community members	

Table 4: Program of 2nd Stakeholder Community meeting

At this meeting, one presentation, in particular, stood out and proved to be a pivotal moment for the CyberSEAS Stakeholder Community. The presentation, delivered among the members, provided crucial insights and laid a solid foundation for the continuation and further development of the community's work. It underscored several key directions and priorities that the members of the CyberSEAS Stakeholder Community identified as essential to address not only during the course of the project but also in the post-project phase.

This presentation served as a catalyst for deepening discussions and fostering collaboration among stakeholders, guiding the strategic focus of the community. It highlighted emerging challenges, innovative approaches, and areas where the community could contribute significantly to advancing cybersecurity within the EPES (Energy, Power, and Energy Systems) sector. Furthermore, it provided a platform for members to express their needs and expectations, ensuring that the project's outcomes would be closely aligned with the real-world demands and future aspirations of the community.

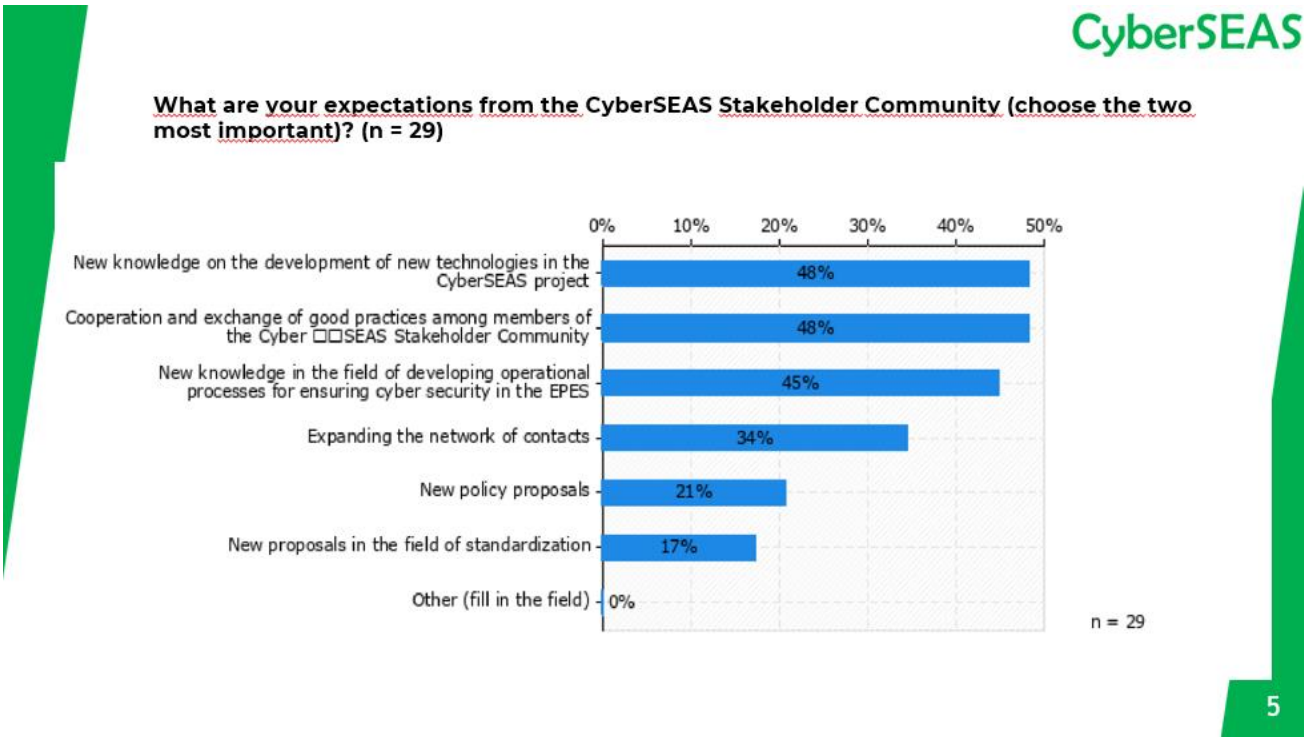
The insights gained from this presentation were instrumental in shaping the roadmap for ongoing activities and set the stage for sustained engagement and collaboration beyond the project's official timeline. This moment marked a significant step forward in building a resilient, forward-thinking community that is well-equipped to tackle the evolving challenges in cybersecurity and critical infrastructure protection.



CyberSEAS

Please indicate from which sector you come from: (n = 29)

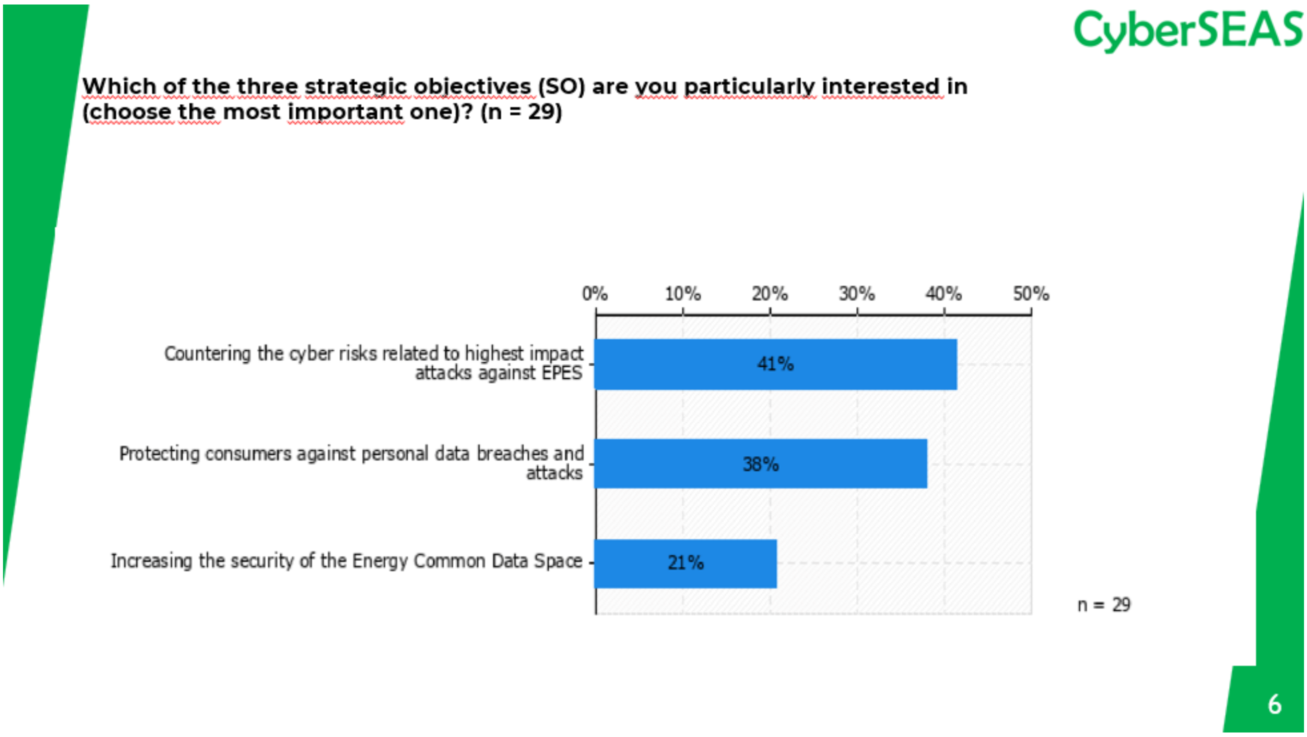
4



CyberSEAS

What are your expectations from the CyberSEAS Stakeholder Community (choose the two most important)? (n = 29)

5



Which of the three strategic objectives (SO) are you particularly interested in (choose the most important one)? (n = 29)

From this research, the results of which were thoroughly presented to the entire community, we have extracted several important aspects for this report.

The third meeting was organized on September 27, 2023

The third meeting of the CyberSEAS Stakeholder Community, which took place during the General Assembly of the CyberSEAS project in Sardinia, represented a key milestone in the project's timeline. Organized as a hybrid event, the meeting allowed for both in-person attendance, particularly from the Advisory Board members, and virtual participation to maximize engagement across the stakeholder community.

This meeting held considerable importance as it provided the first opportunity for the community members to engage with and review the technological advancements and solutions that had been developed by the project partners during the initial phase of the project. The physical presence of the Advisory Board added a layer of significance, facilitating direct, in-depth discussions on the progress made and the potential implications of the new technologies for the broader EPES (Electrical Power and Energy Systems) sector.

The event was not just a showcase of technological developments but also a platform for collaborative dialogue. Participants were encouraged to provide feedback, share their perspectives, and discuss how these innovations could be integrated into their own operational contexts. This interaction was crucial for aligning the project's outputs with the real-world needs and challenges faced by stakeholders within the EPES ecosystem.

Moreover, the hybrid format of the meeting demonstrated the project's commitment to inclusivity and broad participation, ensuring that even those who could not travel to Sardinia could still actively contribute to the discussions and decision-making processes. This approach reinforced the collaborative spirit of the CyberSEAS project, fostering a sense of community and shared purpose among the diverse group of stakeholders involved. The third meeting of the CyberSEAS Stakeholder Community was a pivotal event that not only highlighted the project's technological progress but also strengthened the collaborative ties among stakeholders, setting the stage for the successful continuation and eventual completion of the project's goals.

Time	**Presentation**	**Presenter**	
14:00-14.05	Welcome and introduction	Dr. Denis Caleta	
14:05-14:30	Demo Introduction and Technical recap (main technical/scientific results)	Dr. Luigi Romano (CINI)	
14:30-14:55	Demo session 1 (Business Process IDS – Demonstration)	Dr. Luigi Coppolino (CINI), Mrs. Cristina Barbero (BER)	
14:55-15:20	Demo session 2 (ALIDA solution for Social Engineering) – (25 minutes)	Mr. Davide Profeta (ENG+ENERIM)	
14:20-15:45	Demo session 3 (MIDA tool demo supports supply chain security risk mitigation highlighted in NIS 2 directive) - (25 minutes)	Dr. Priit Anton (GT)	
15:45-16:30	Discussion and proposals from CyberSEAS Stakeholder members	All community members	

Table 5: Program of 3th Stakeholder Community meeting

The feedback obtained from participants at the meeting provided essential and highly valuable insights for the continuation of the project. These insights were particularly crucial for aligning the project's trajectory with the immediate needs of the real-world environment. To gain a more detailed understanding of the feedback, we developed a survey questionnaire, which was later distributed to the attendees who participated in the presentation of the first set of tools developed under the CyberSEAS project.

In the following section, we present some key aspects that were analysed based on the feedback received.

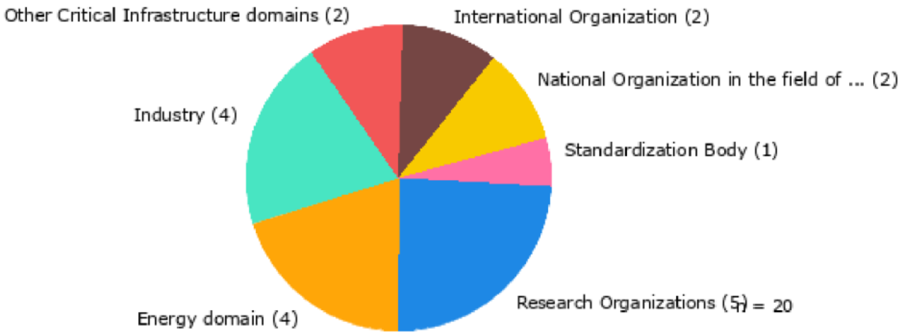
CyberSEAS Survey for Stakeholder community members – Olbia meeting 27.09.2023

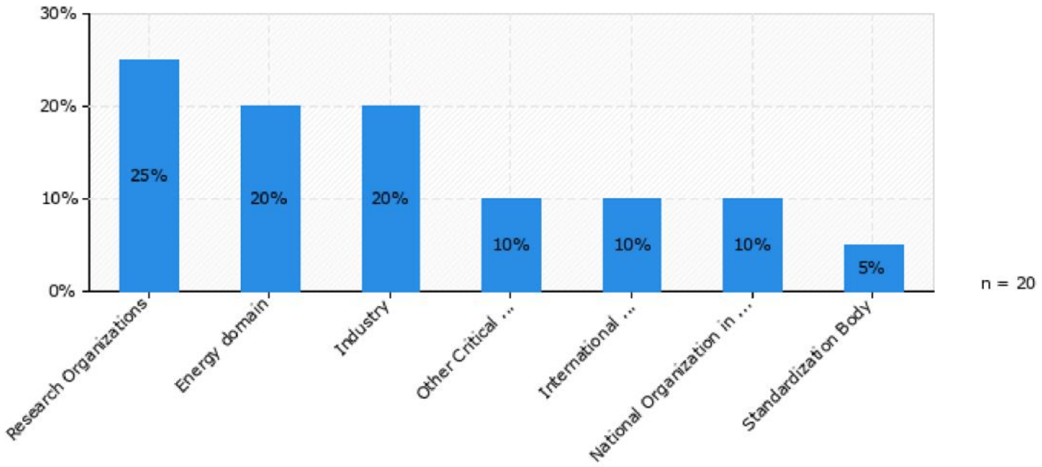
The mentioned survey was conducted during a consortium partners meeting in Olbia, Sardinia. As part of this program, a specific section was dedicated to presenting new technological solutions developed within the CyberSEAS project. The presentation was intended for the CyberSEAS Stakeholder group and representatives of the Advisory Board. The following three tools were presented:

- Business Process IDS – Demonstration
- ALIDA solution for Social Engineering
- MIDA tool demo supports supply chain security risk mitigation highlighted in NIS 2 directive.

The main summary of the analysed responses is provided below:

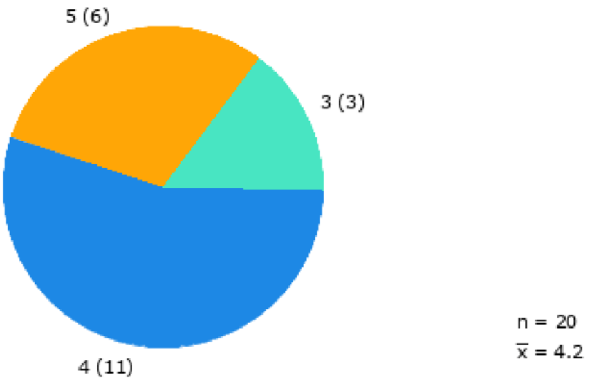
1. **Please indicate from which sector you come from.**

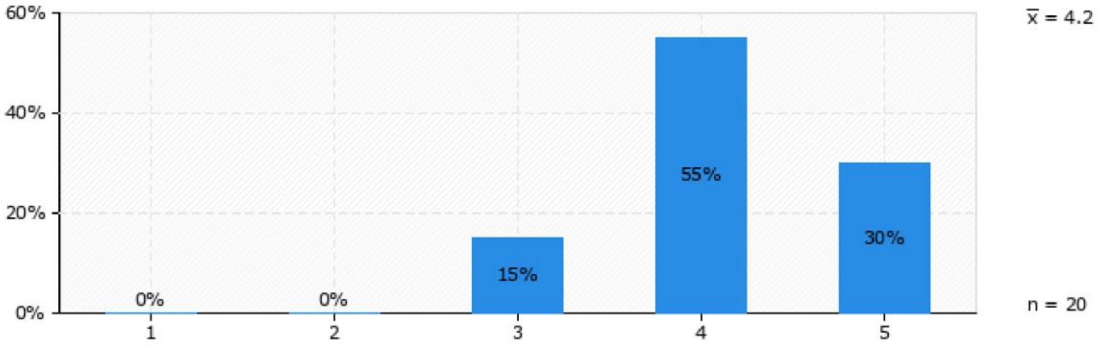




From the answers we can see that 25% of the respondents come from the Research Organization, 20% from the Energy domain, 20% from the industry sector, 10% from the Other Critical Infrastructure Domains sector, 10% of the respondents are from the International Organization, 10% of the respondents come from the National Organization in the field of (policy, legislation, security) and 5% from the Standardization Body.

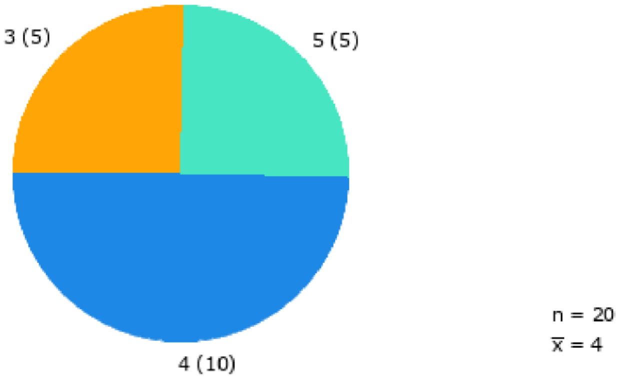
2. **Do you personally see technological value of a CyberSEAS presented technology approaches for ensuring a higher level of cyber security? (Quantify the value (1-5)**

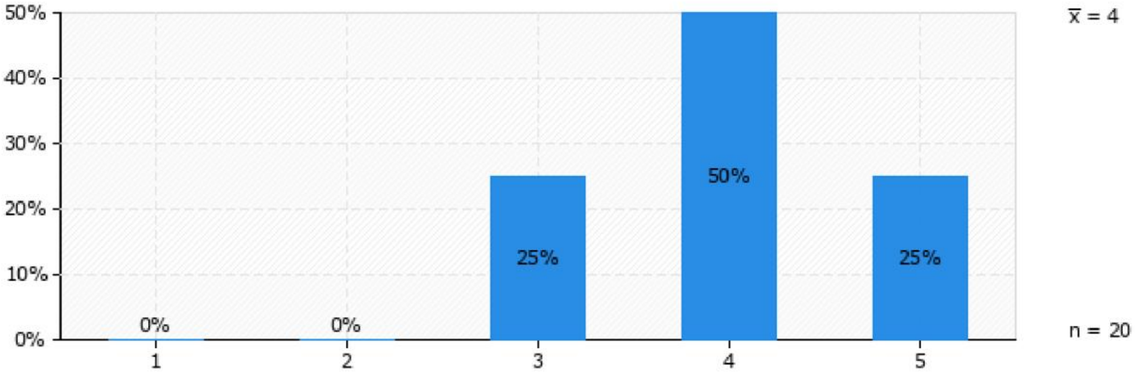




In response to the question "Do you personally see technological value of a CyberSEAS presented technology approaches for ensuring a higher level of cyber security", six respondents chose the value 5, eleven responders chose the value 4 and three chose the value 3.

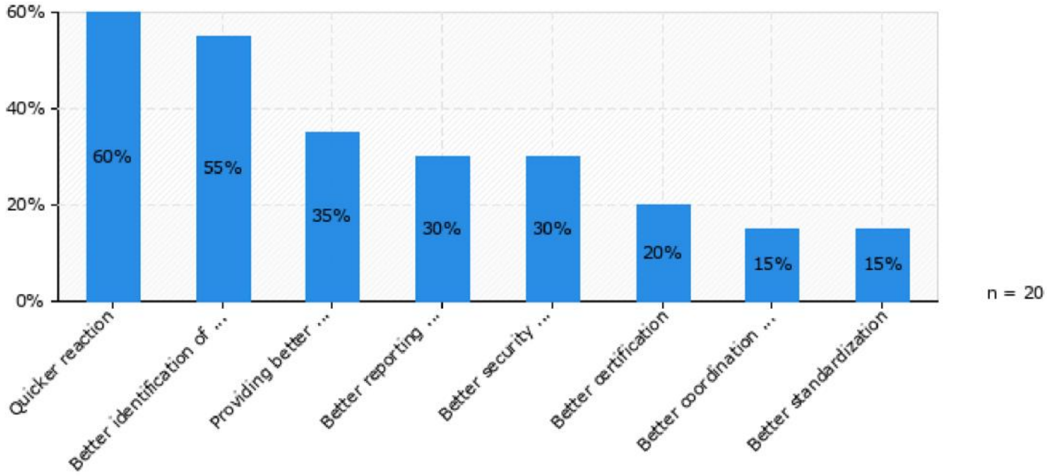
3. **How much the CyberSEAS tool (Intrusion detection system (IDS) can contribute to improve the security of EPES in daily life scenarios? (Quantify the value (1-5) od tool according to your experience. Answers are valued 1-low, 5-high.)**





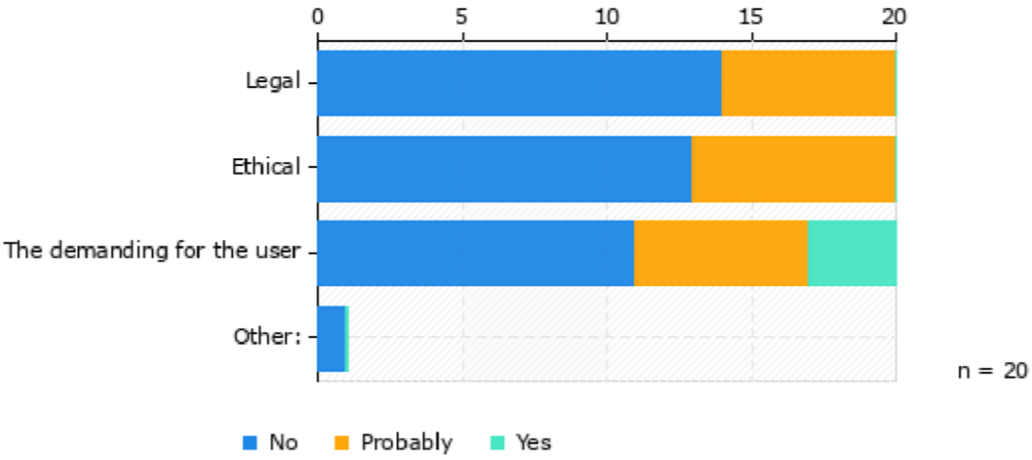
In response to the question " How much the CyberSEAS tool (Intrusion detection system (IDS) can contribute to improve the security of EPES in daily life scenarios ", five respondents chose the value 5, ten responders chose the value 4 and five chose the value 3.

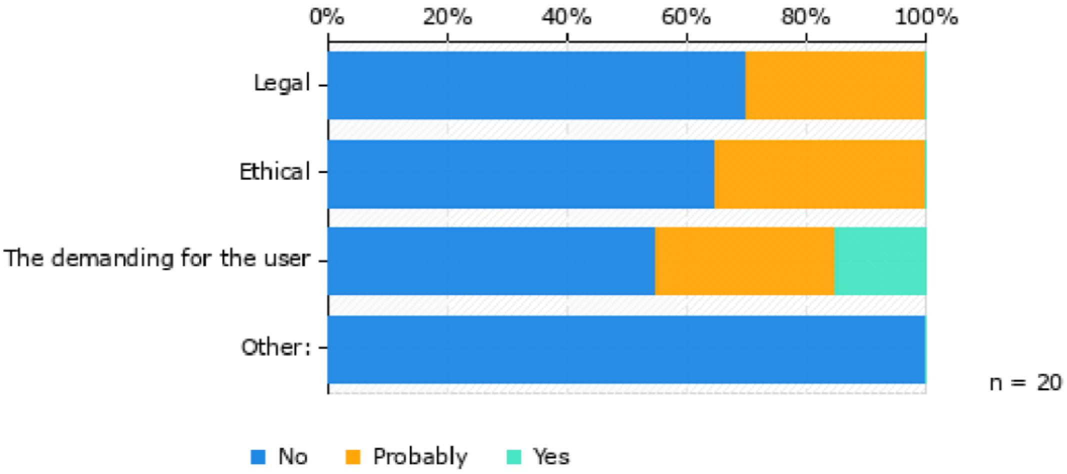
4. In which specific area of ensuring Cyber Security in EPES do the IDS tool provide



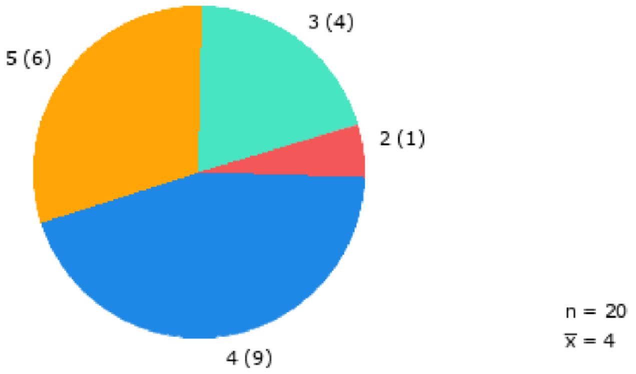
When we asked, " In which specific area of ensuring Cyber Security in EPES do the IDS tool provide added value ", 12 chose quicker reaction, 11 chose better identification of cybersecurity threats, 7 chose providing better operational picture, 6 chose better reporting processes, 6 also chose better security awareness of personnel, 4 chose better certification, 3 chose better coordination of activities among different points in system of cybersecurity and 4 chose better standardization.

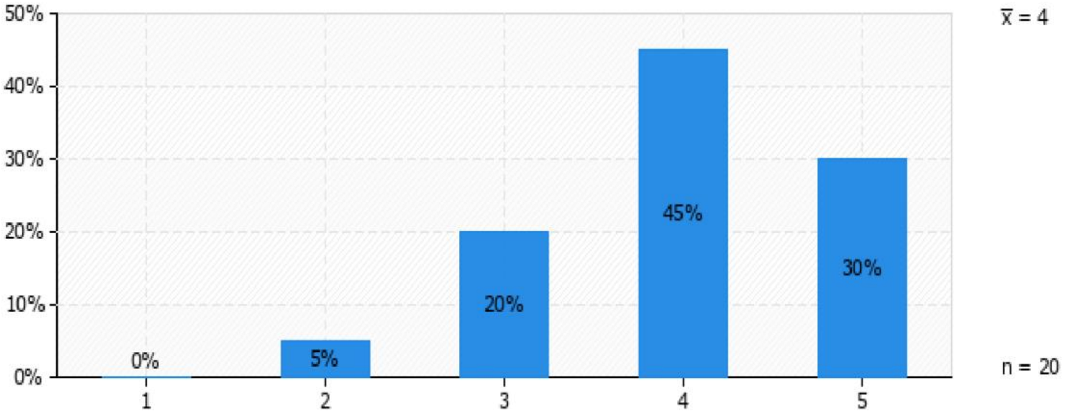
5. **Do you see any limitations for using the IDS tool?**





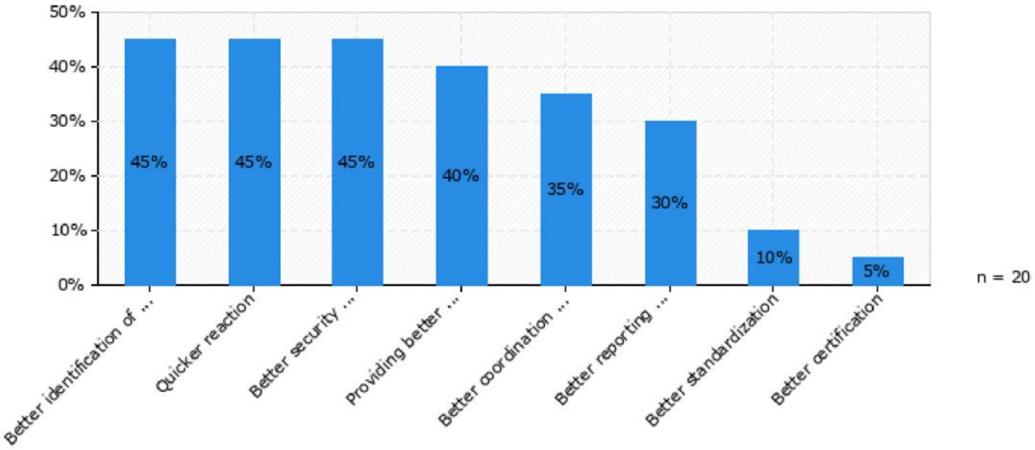
6. **How much the CyberSEAS tool (ALIDA – for Social engineering) can contribute to improve the security of EPES in daily life scenarios? (Quantify the value (1-5) od tool according to your experience. Answers are valued 1-low, 5-high.)**





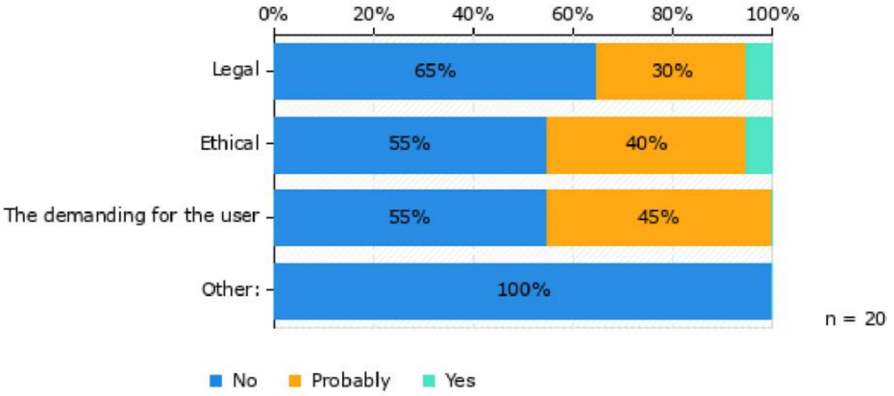
In response to the question " How much the CyberSEAS tool (ALIDA – for Social engineering) can contribute to improve the security of EPES in daily life scenarios", six respondents chose the value 5, nine responders chose the value 4, four responders chose the value 3 and two chose the value 1.

7. In which specific area of ensuring Cyber Security in EPES do the IDS tool provide added value?

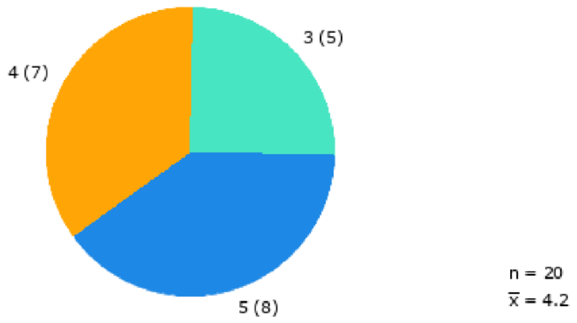


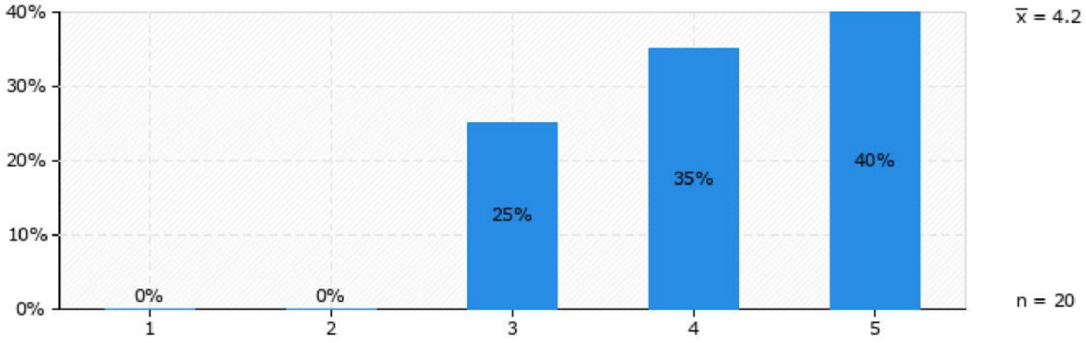
When we asked, " In which specific area of ensuring Cyber Security in EPES do the IDS tool provide added value ", 9 chose quicker reaction, 9 chose better identification of cybersecurity threats, 9 chose better security awareness of personnel, 8 chose providing better operational picture, 7 chose better coordination of activities among different points in system of cybersecurity, 6 chose better reporting processes, 2 chose better standardization and 1 chose Better certification.

8. Do you see any limitations for using the ALIDA tool?



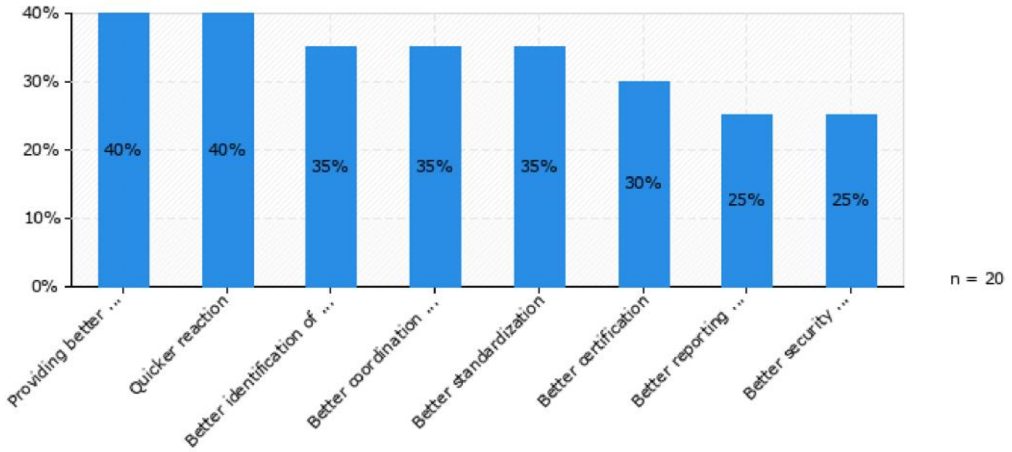
9. How much the CyberSEAS tool (MIDA tool demo supports supply chain security risk mitigation highlighted in NIS 2 directive) can contribute to improve the security of EPES in daily life scenarios? (Quantify the value (1-5) od tool according to your experience. Answers are valued 1-low, 5-high.)





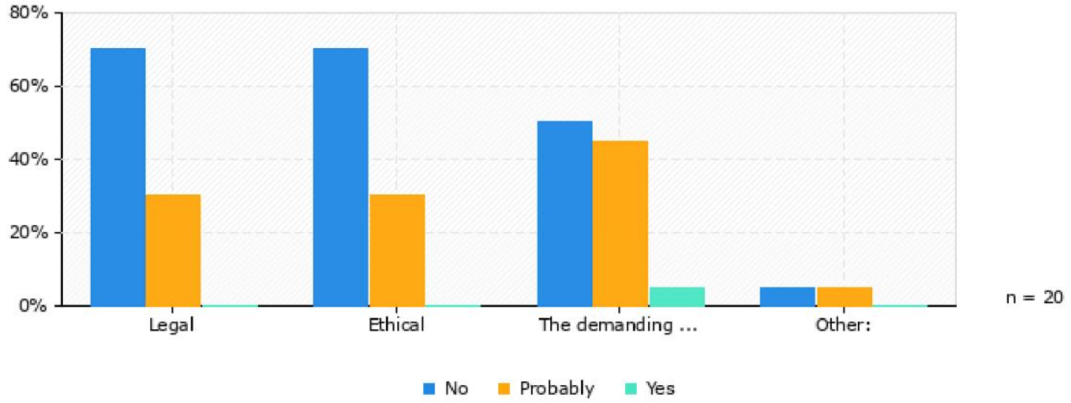
In response to the question "How much the CyberSEAS tool (MIDA tool demo supports supply chain security risk mitigation highlighted in NIS 2 directive) can contribute to improve the security of EPES in daily life scenarios ", eight respondents chose the value 5, seven responders chose the value 4 and five responders chose the value 3.

10. In which specific area of ensuring Cyber Security in EPES do the MIDA tool provide added value?



When we asked, "In which specific area of ensuring Cyber Security in EPES do the MIDA tool provide added value", 8 chose providing better operational picture, 8 also chose quicker reaction, 7 chose better identification of cybersecurity threats, 7 chose better coordination of activities among different points in system of cybersecurity, 7 also chose better standardization, 6 chose Better certification, , 5 chose better reporting processes and 5 chose better security awareness of personnel.

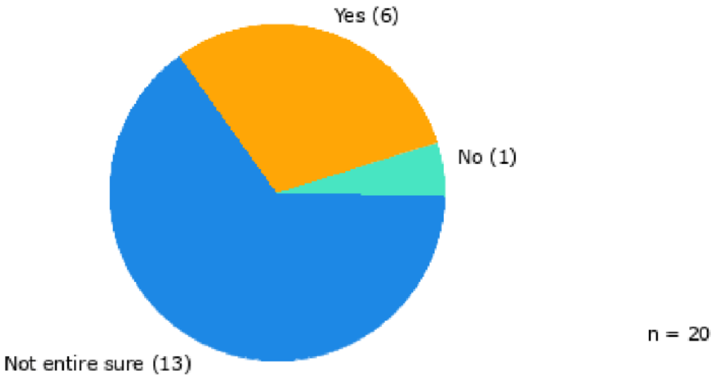
11. Do you see any limitations for using the MIDA tool?

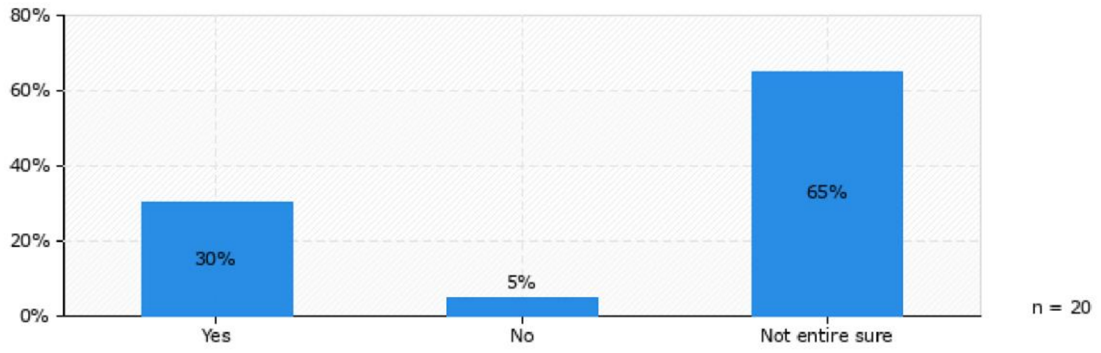


11.a. (Other):

- operational

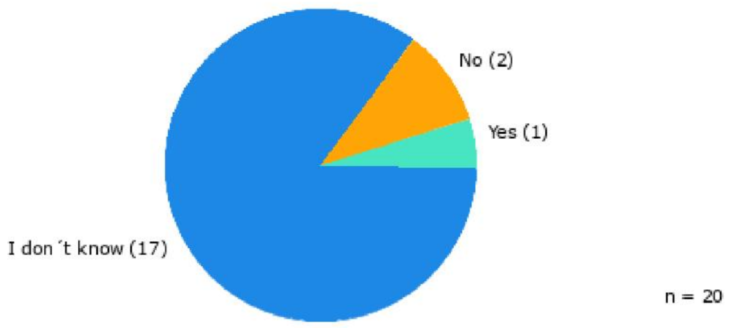
12. Do you clearly understand which data's does the technological solution need for effective operation?

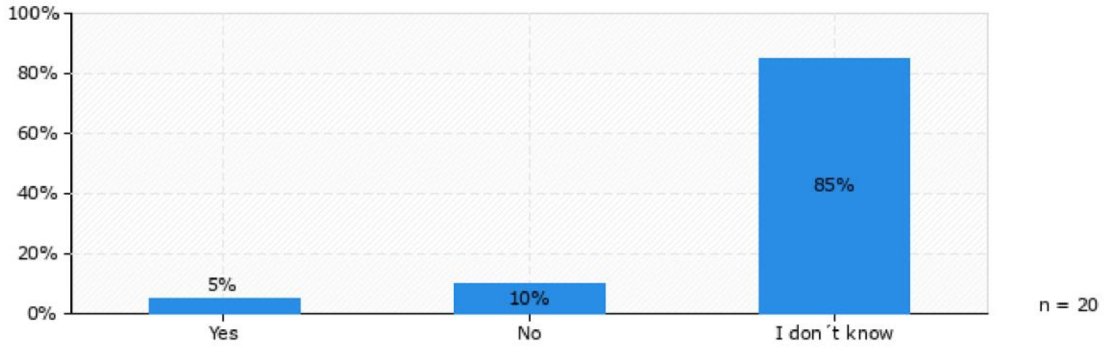




Of the twenty respondents, 6 answered yes, 1 answered no and 13 answered not entirely sure.

13. Are there tools on the market that provide similar technological solutions?



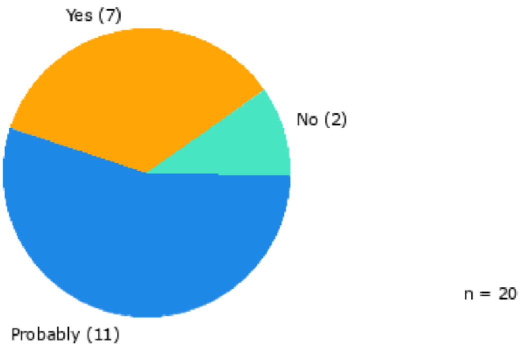


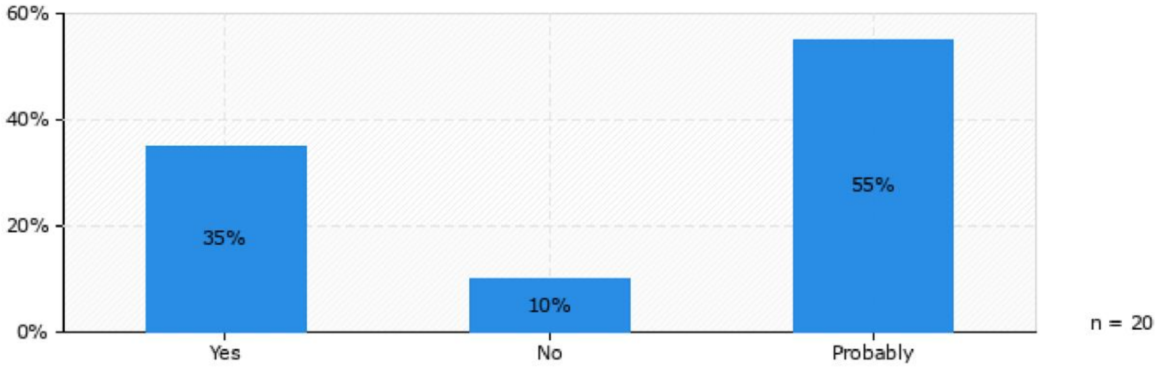
When asked »Are there tools on the market that provide similar technological solutions«, 1 answered yes, 2 answered no and 17 chose don't know.

13.a. If you selected YES in the previous question, please give some examples.

- verifiable data from the source (meter point, software developer git, logs). there are multiple tools for social media data collection that can be implemented with crm. utility can use signing software as an alternative.

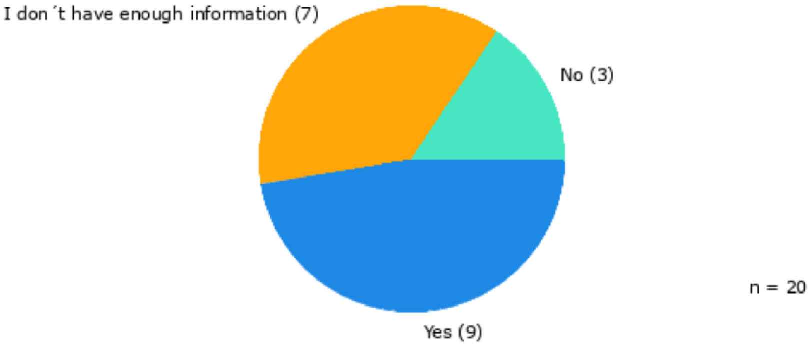
14. Is it possible to integrate the tool with other technological solutions that are already implemented in cyber security assurance systems in EPES?

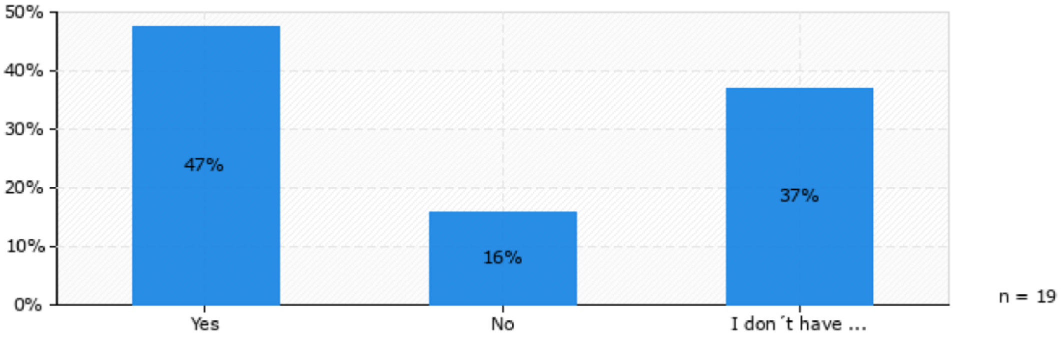




To the question "Is it possible to integrate the tool with other technological solutions that are already implemented in cyber security assurance systems in EPES", seven answered yes, two answered no and eleven answered probably.

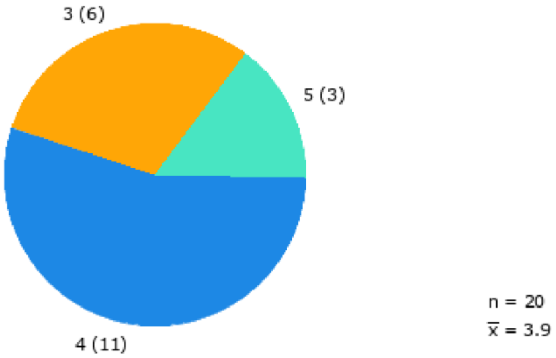
15. Is the use of the technological solution possible only for cyber experts with a high level of knowledge?

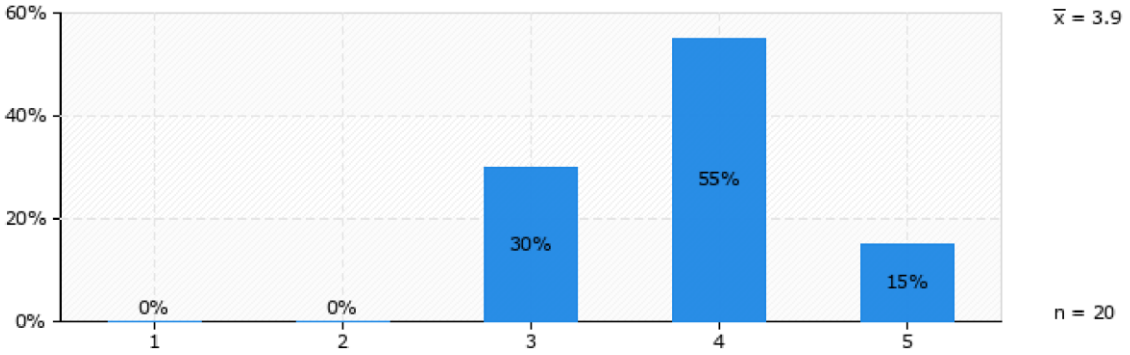




To the question "Is the use of the technological solution possible only for cyber experts with a high level of knowledge", nine answered yes, three answered no and seven answered i don´t have enough information.

16. Do you see some commercial possibility for tools presented in the meeting? (Quantify the value (1-5) each of presented tools according to your experience. Answers are valued 1-low, 5-high).





In response to the question "Do you see some commercial possibility for tools presented in the meeting", three respondents chose the value 5, eleven responders chose the value 4 and six responders chose the value 3.

4th Stakeholder Community meeting – 07. MARCH 2024 11:00-13:45 (on-line)

The fourth meeting of the CyberSEAS Stakeholder Community, conducted online, represented a pivotal moment in the project's timeline, marking a progression in both scope and depth of the discussions. The meeting did not just continue the conversation around technological advancements but expanded to cover crucial improvements in process and methodological approaches within the cybersecurity domain, specifically tailored to the needs of the EPES sector.

In this session, for the first time, participants were introduced to preliminary insights from WP6 (Cyber Secure Energy Common Data Space) and WP8 (Fostering the Culture of Cyber-Resilient Energy Supply Chain). These work packages are central to the project's goals of creating a more secure and resilient energy sector, and their inclusion in the discussion underscored the broadening focus of the project from mere technological innovation to encompassing comprehensive cybersecurity strategies.

Moreover, the meeting featured a dedicated session organized by the Market Interest Group (MIG). This session was particularly significant as it offered a platform for integrating market-oriented perspectives into the project’s ongoing developments. The discussions within MIG provided valuable insights into the commercial viability and potential exploitation of the tools and solutions being developed. By bringing together technical experts, market analysts, and stakeholders, the session ensured that the project’s outcomes are not only technically sound but also aligned with market needs and future exploitation opportunities.

The meeting concluded with a strong emphasis on the importance of aligning the project’s innovations with real-world applications and market demands, ensuring that the solutions developed are both practically applicable and commercially viable. This comprehensive approach reflects the project's commitment to not only advancing technological capabilities but also fostering a robust market ecosystem that supports the long-term sustainability and adoption of these solutions across the energy sector.

Additionally, a dedicated segment of the meeting was reserved for showcasing the activities related to the **Women in Cyber** initiative within the project. Female colleagues involved in the project presented their efforts and contributions in this area, highlighting both their individual roles and the broader impact of their work. They also discussed the connections and collaborations that the project established with other international **Women in Cyber** initiatives.

This presentation underscored the project's commitment to promoting diversity and inclusion in the cybersecurity field, not just within the project itself, but also by engaging with and supporting global movements aimed at empowering women in this critical sector. The integration of these perspectives was essential in fostering a more inclusive approach to cybersecurity, ensuring that diverse voices are represented and that the solutions developed are more comprehensive and resilient.

Time	**Presentation**	**Presenter**	
11:00-11.05	Welcome and introduction	Denis Caleta (ICS)	
11:05-11:25	Main steps in evolution of CyberSEAS project (approaching the last phase)	Paolo Roccetti (ENG)	
11:25-11:45	Assessing Cyber Risks for Operational Technologies in the EPES domain	Paolo Roccetti Maurizio Casciano (ENG)	
11:45-12:05	Preparation plan for Data breach incident – CyberSEAS best practice	Janne Huvilinna (Enerim)	
12:05-12:25	ARTEMIS and Attack Defense Simulator working together on the EST pilot	Konstantinos Lessis (WINGS) , Abraham Ezema (RWTH)	
12:25-12:45	Introducing CyberSEAS's Learning Management System	Alexandru Pirojoc (SIMAVI)	
12:45-13:20	Market Interest Group (MIG) panel discussion. - TSO representative, from the SCC (Security Coordination Center) from Serbia – Dusan	Mihai Mladin (CRENERG)	

	Presic – Assistant Director for Development - DSO representative, from Israel Electric Corporation – Elad Shaviv – Director of Markets and Business Development - Cybersecurity solutions provider targeting EPES specifically – Enersec Company – Andrei Hohan – Managing Partner		
13:20-13:30	Notification of next steps for initiative in CyberSEAS "Women in Cyber"	Maja Horvat (SI-CERT)	
13:30-13:45	Discussion and proposals for the next meeting	All community members	
	Conclusion of the meeting		

Table 6: Program of 4th Stakeholder Community meeting

CyberSEAS third Survey for Stakeholder community members – 07. MARCH 2024

As we have established in previous joint meetings of the CyberSEAS Stakeholder Group, following the presentations and discussions, we requested that participants complete a prepared questionnaire. This approach allowed us to gather valuable insights, feedback, and additional indicators, which served as crucial guiding factors for the project's ongoing development. The feedback collected is not only essential for assessing the relevance and practicality of the presented technologies and process methodologies from the perspective of CyberSEAS Stakeholder community members but also plays a significant role in shaping the overall direction of the project.

The continuous practice of soliciting detailed feedback through these questionnaires ensures that the technologies, tools, and process approaches introduced during the meetings are not just theoretically sound but also practically applicable and aligned with the real-world needs and challenges faced by stakeholders in the energy and cybersecurity sectors. This feedback loop has become a cornerstone of our methodology, providing an ongoing assessment of how well the project meets the dynamic and evolving needs of its diverse stakeholders.

Moreover, these questionnaires have proven instrumental in encouraging active participation during the meetings. By ensuring that community members know their insights are valued and will influence the project's trajectory, we have fostered a more engaged and committed stakeholder community. This engagement is particularly important as it leads to more robust discussions, richer exchanges of ideas, and more actionable feedback, all of which contribute to refining the project's outputs and ensuring they are fit for purpose.

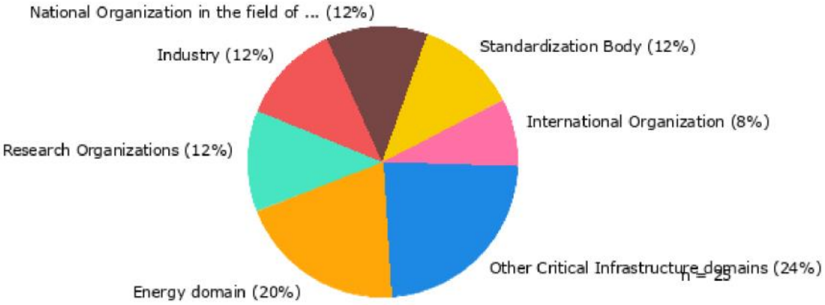
In addition to enhancing participation, the questionnaires serve a dual purpose by providing a mechanism for continuous improvement. They enable us to identify gaps in understanding, areas where further clarification or development is needed, and emerging needs that may not have been initially anticipated. This process of continuous feedback and iterative improvement is critical for maintaining the project's relevance and ensuring its outputs are as effective and impactful as possible.

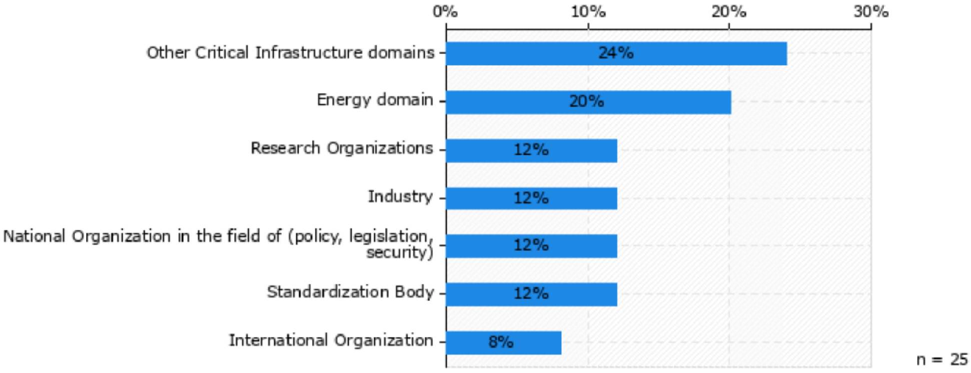
Furthermore, this structured approach to feedback collection and analysis has allowed us to build a comprehensive understanding of the varying needs across different sectors represented within the CyberSEAS Stakeholder Group. It has highlighted the unique challenges faced by different stakeholders, enabling us to tailor our solutions more precisely to address these challenges. This targeted approach not only enhances the effectiveness of the solutions developed but also ensures that they are scalable and adaptable to different contexts and environments.

Practice of requesting feedback through questionnaires following meetings has become an integral part of our stakeholder engagement strategy. It ensures that the project remains closely aligned with stakeholder needs, fosters active participation, and provides a continuous mechanism for improving the project's outcomes. By closely monitoring and responding to the feedback received, we are able to steer the project in a direction that maximizes its impact and relevance to the real-world challenges of the energy and cybersecurity sectors.

The main summary of the analysed responses is provided below:

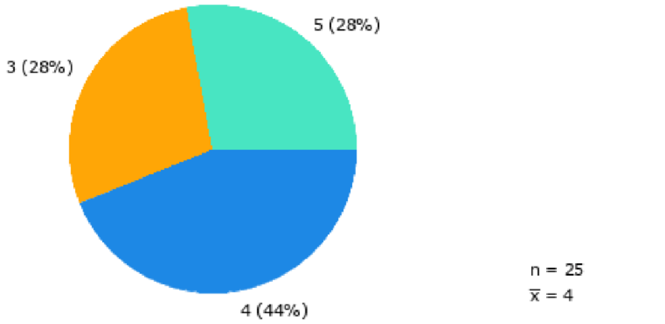
1. **Please indicate from which sector you come from.**

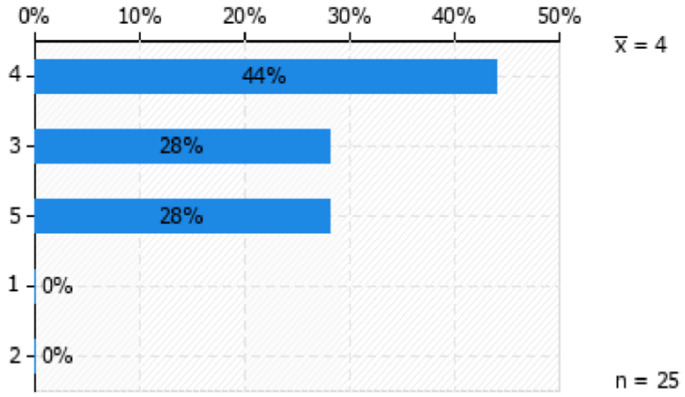




From the answers we can see that 24% of the respondents come from the Other Critical Infrastructure Domains sector, 20% from the Energy domain, 12% from the Research Organizations, 12% from the industry sector, 12% from the National Organization in the field of (policy, legislation, security), 12% of the respondents are from the Standardization Body and 8% from the International Organization.

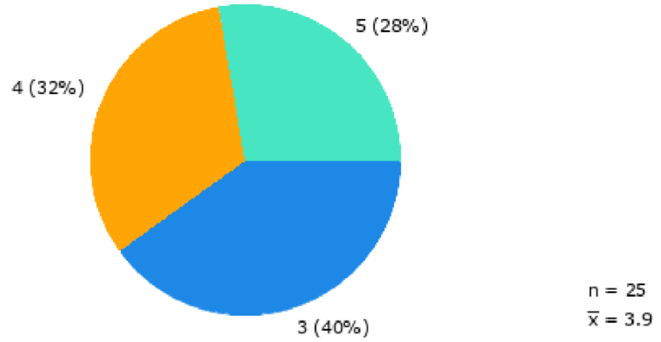
2. **How much the assessing Cyber Risks for Operational Technologies in the EPES domain can contribute to improve the security of EPES in daily life scenarios? (Quantify the value (1-5) od tool according to your experience. Answers are valued 1-low, 5-high.)**

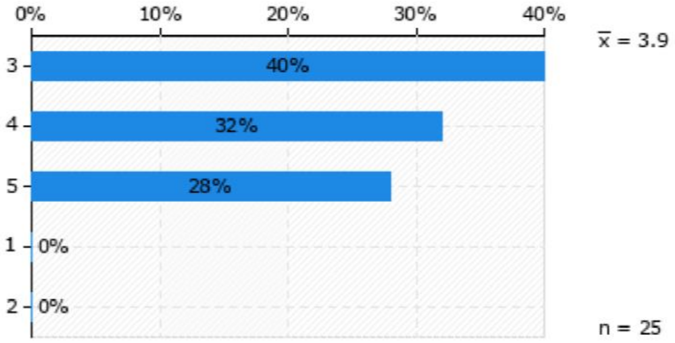




In response to the question "How much the assessing Cyber Risks for Operational Technologies in the EPES domain can contribute to improve the security of EPES in daily life scenarios?", 28% respondents chose the value 5, 44% respondents chose the value 4 and 28% chose the value 3.

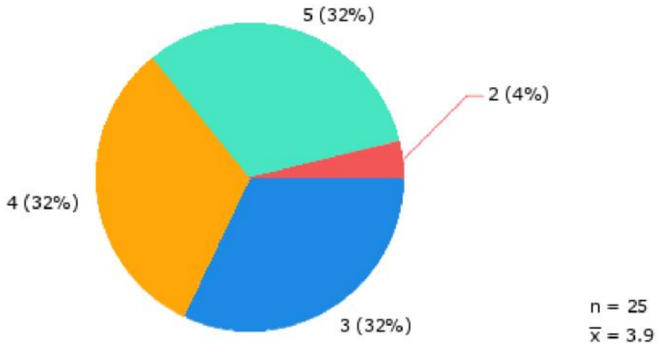
3. **How much the CyberSEAS's Learning Management System can contribute to improve the security of EPES in daily life scenarios? (Quantify the value (1-5) od tool according to your experience. Answers are valued 1-low, 5-high.)**

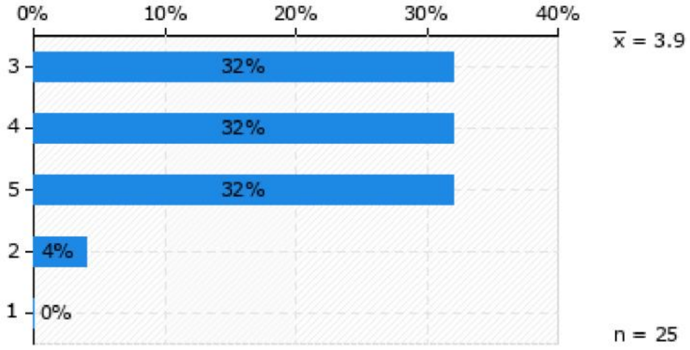




In response to the question "How much the CyberSEAS's Learning Management System can contribute to improve the security of EPES in daily life scenarios?", 28% respondents chose the value 5, 32% respondents chose the value 4 and 40% chose the value 3.

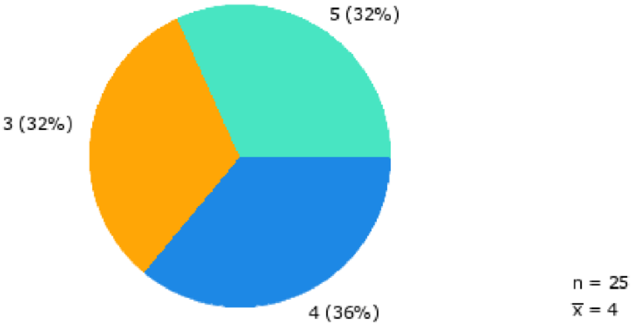
4. **How much the preparation plan for Data breach incident can contribute to improve the security of EPES in daily life scenarios? (Quantify the value (1-5) od tool according to your experience. Answers are valued 1-low, 5-high.)**

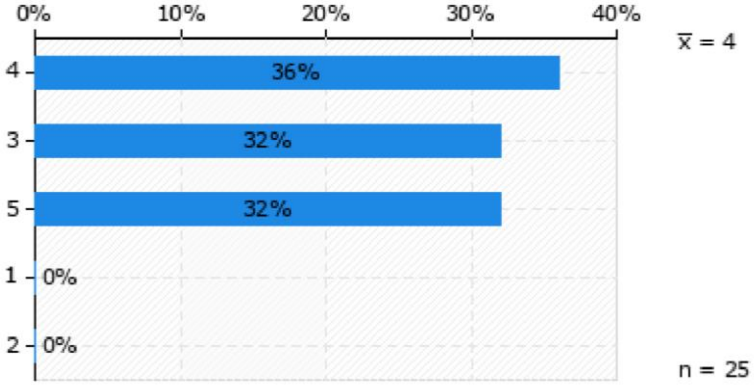




In response to the question "How much the preparation plan for Data breach incident can contribute to improve the security of EPES in daily life scenarios?", 32% respondents chose the value 5, 32% respondents chose the value 4, 32% respondents chose the value 3 and 4% chose the value 2.

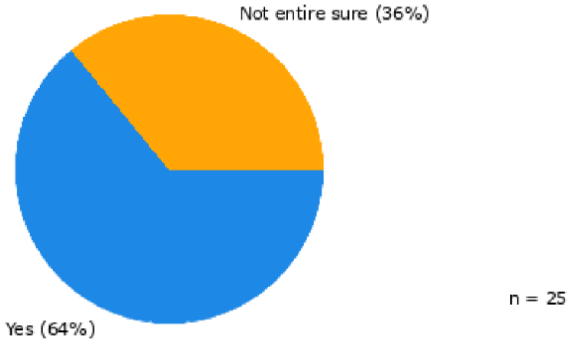
5. **Do you personally see technological value of a CyberSEAS presented technology approaches for ensuring a higher level of cyber security? (Quantify the value (1-5) according to your experience. Answers are valued 1-low, 5-high.)**

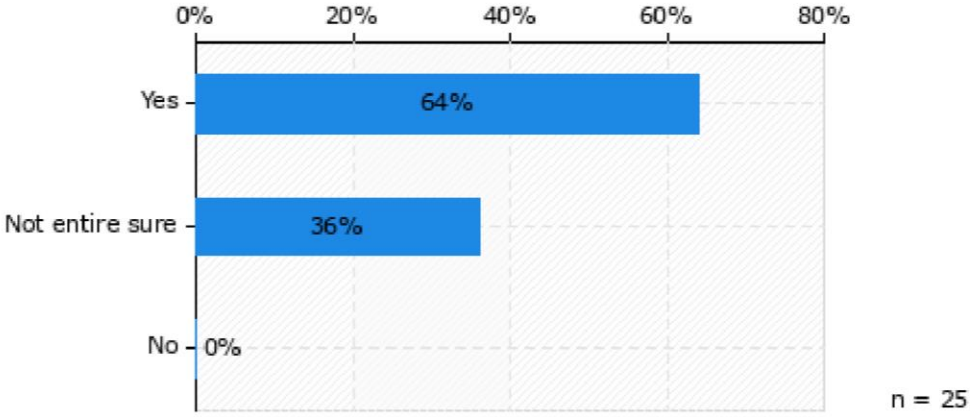




In response to the question "Do you personally see technological value of a CyberSEAS presented technology approaches for ensuring a higher level of cyber security?", 32% respondents chose the value 5, 36% respondents chose the value 4, 32% respondents chose the value 3.

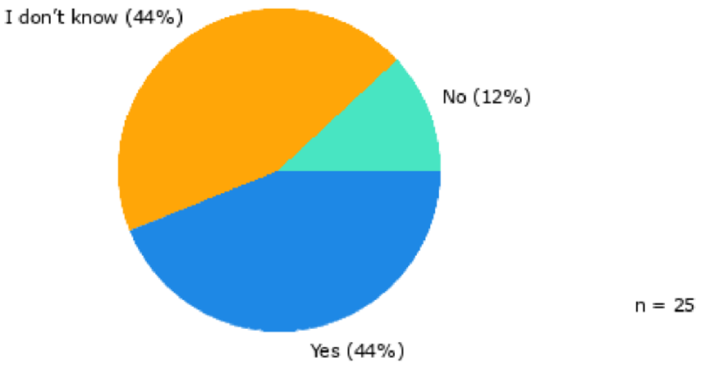
6. **Do you clearly understand which data's does the technological solution need for effective operation?**

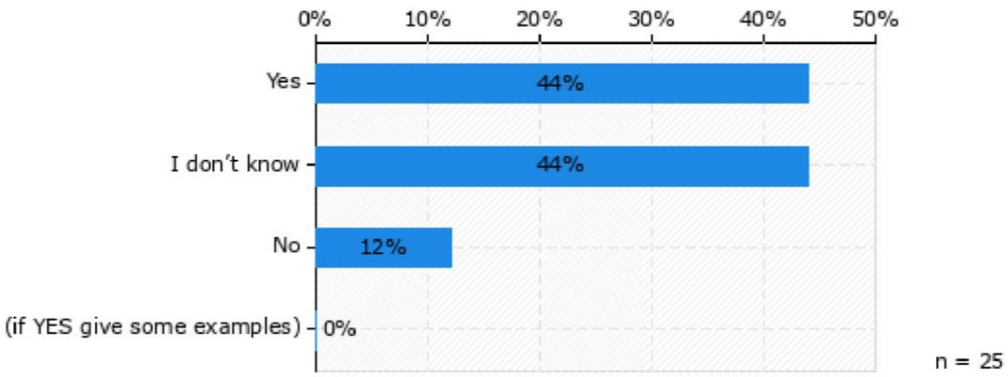




In response to the question "Do you clearly understand which data's does the technological solution need for effective operation?", 64% respondents chose the answer Yes and 36% respondents chose the answer Not entire sure.

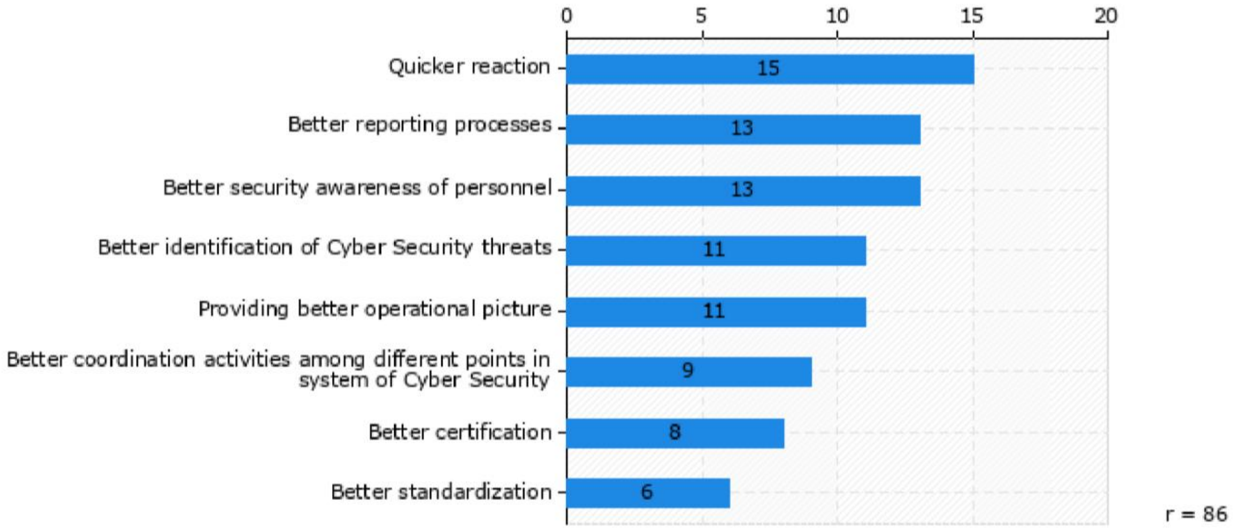
7. **Are there tools on the market that provide similar technological solutions?**





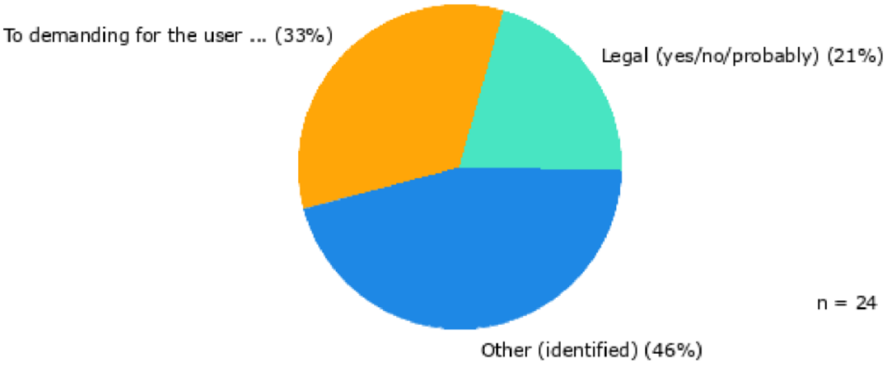
In response to the question "Are there tools on the market that provide similar technological solutions?", 44% respondents chose the answer Yes, 44% respondents chose the answer I don't know and 12% respondents chose the answer No.

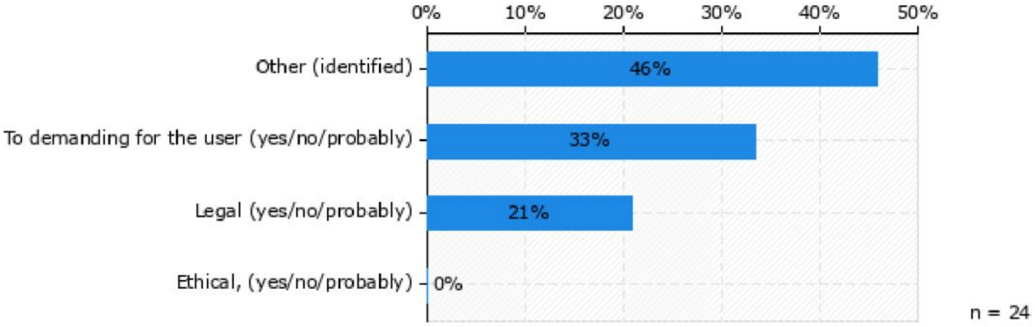
8. In which specific area of ensuring cyber security in EPES does the tool provide added value?



When we asked, "In which specific area of ensuring cyber security in EPES does the tool provide added value?", 15 chose quicker reaction, 13 chose better reporting processes, 13 chose better security awareness of personnel, 11 chose better identification of Cyber Security threats, 11 chose providing better operational picture, 9 chose better coordination activities among different points in system of Cyber Security, 8 chose better certification and 6 chose better standardization.

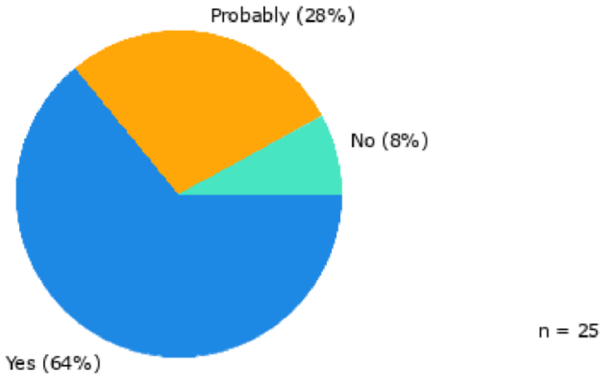
9. Do you see any limitations for using the tool?

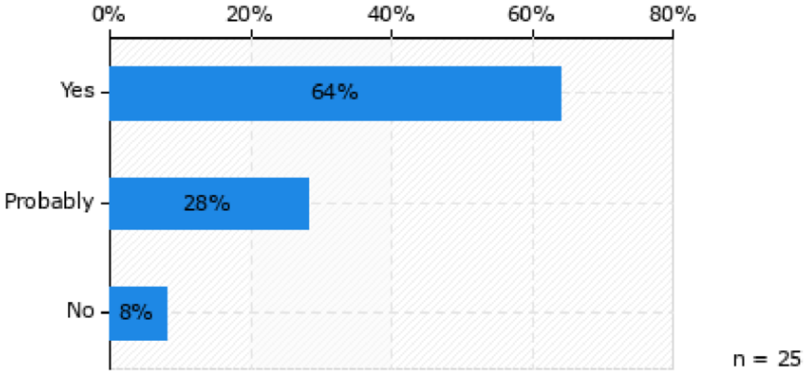




In response to the question "Do you see any limitations for using the tool?", 46% respondents chose the answer Other, 33% respondents chose the answer to demanding for the user and 21% respondents chose the answer Legal.

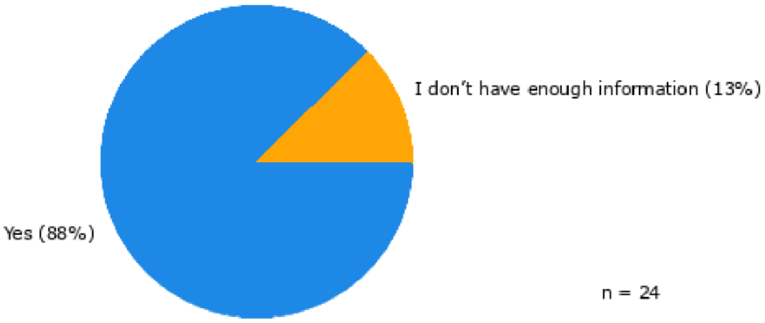
10. Is it possible to integrate the tool with other technological solutions that are already implemented in cyber security assurance systems in EPES?

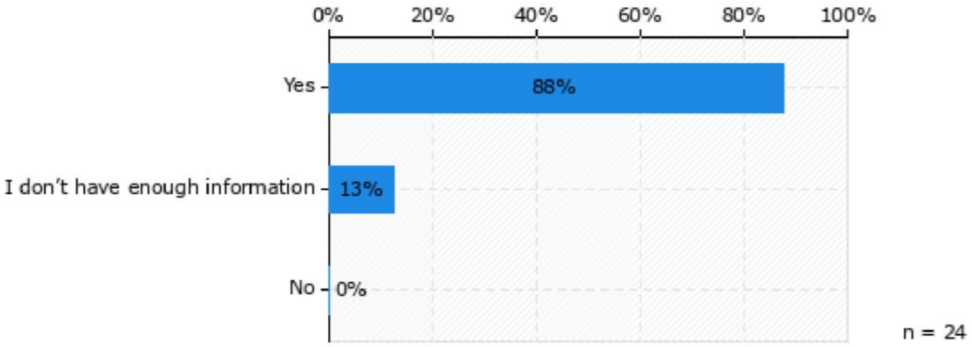




In response to the question "Is it possible to integrate the tool with other technological solutions that are already implemented in cyber security assurance systems in EPES?", 64% respondents chose the answer Yes, 28% respondents chose the answer Probably and 8% respondents chose the answer No.

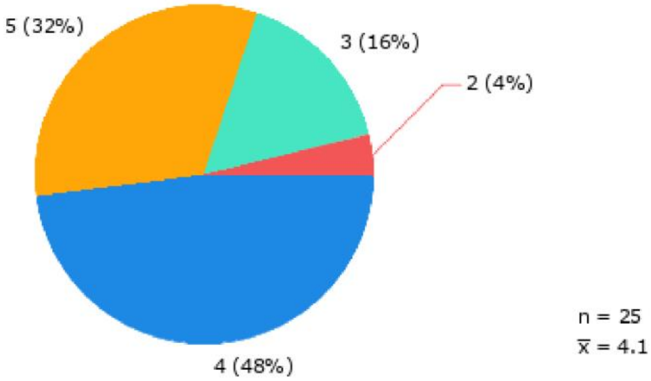
11. Is the use of the technological solution possible only for cyber experts with a high level of knowledge?

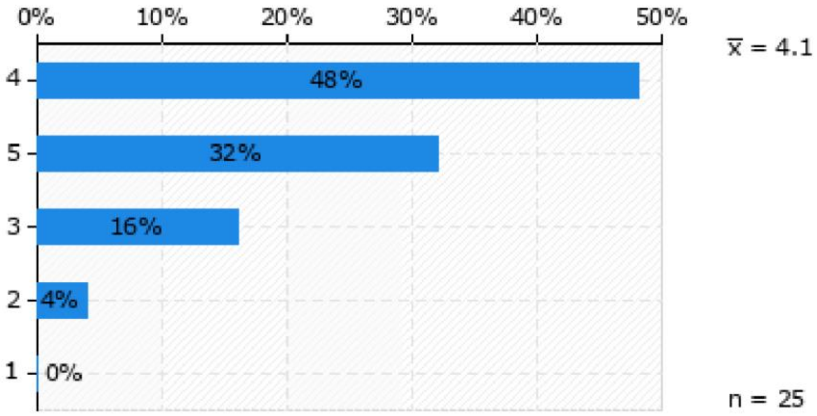




When we asked, "Is the use of the technological solution possible only for cyber experts with a high level of knowledge?", 88% chose Yes and 13% chose I don't have enough information.

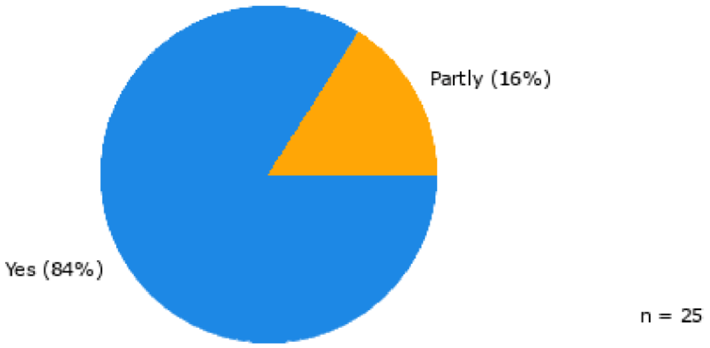
12. Do you see some commercial possibility for tools presented in the meeting. (Quantify the value (1-5) each of presented tools according to your experience).

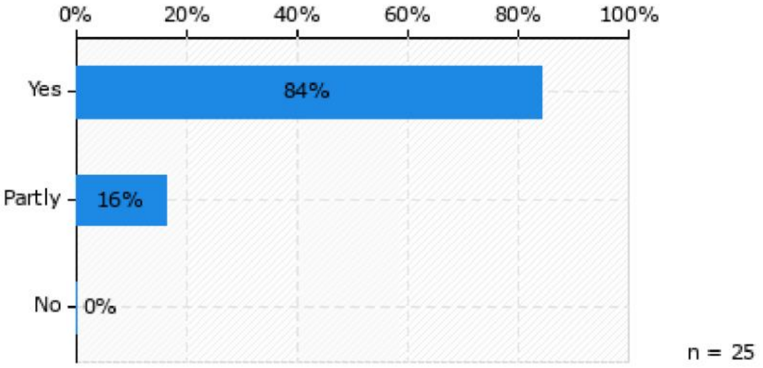




In response to the question "Do you see some commercial possibility for tools presented in the meeting?", 32% respondents chose the value 5, 48% respondents chose the value 4, 16% respondents chose the value 3 and 4% respondents chose the value 2.

13. Do you think Women4Cyber is important?





In response to the question "Do you think Women4Cyber is important?", 84% respondents chose the answer Yes and 16% respondents chose the answer Partly.

5th Stakeholder Community meeting – 29. MAY 2024 10:00-13:00 (on-line)

At the fifth meeting of the CyberSEAS Stakeholder Community, we dedicated special attention to the experiences and detailed information related to the preparation and initial implementation of complex pilots within the project. In addition to continuing presentations on the steps taken in the project and the technologies developed, a significant portion of this meeting was also devoted to discussions and the sharing of feedback, opinions, and experiences from the members of the CyberSEAS Stakeholder Community.

To kick off the in-depth discussion, we invited relevant experts to lead the conversation within the framework of the Market Interest Group (MIG). These experts provided valuable insights and perspectives that helped to set the stage for a broader exchange of ideas among all participants. This approach allowed us to delve into the practical challenges and opportunities encountered during the pilots, ensuring that the discussion was rooted in real-world experiences.

The continuation of the meeting was then opened up to all members of the group, providing them with the opportunity to share their views, opinions, and recommendations. This inclusive discussion format not only facilitated a richer dialogue but also ensured that the diverse perspectives within the community were fully represented and considered.

The feedback and insights gathered during this meeting were particularly valuable for refining the project's ongoing activities, especially in relation to the complex pilots. The direct input from stakeholders who are actively engaged in or affected by the project’s developments enabled us to better align our efforts with the practical needs and expectations of the community. Moreover, the exchange of experiences among members also fostered a deeper understanding of the challenges and best practices, contributing to the overall success of the project.

Here are the key feedback points we received from participants through the discussions:

1. **Usability of Technological Solutions**: Most participants expressed satisfaction with the developed technological solutions and their potential to enhance cybersecurity within energy systems. They particularly highlighted the ease of integration with existing systems and the clear design of user interfaces. Some suggested additional functionalities that could further increase the usability of the solutions, especially in the areas of process automation and better adaptability to the specific needs of individual organizations.
2. **Implementation Challenges**: Participants pointed out potential challenges in implementing the presented solutions in existing operational environments. The main concerns included compatibility with existing systems, the need for additional staff training, and the provision of ongoing support from developers. They also emphasized the importance of the robustness of solutions in the context of diverse infrastructure and security standards already used by organizations.
3. **Importance of Market Adaptation**: Participants stressed the need for developers to consider the specific needs of different market segments during the marketing phase. The need for greater flexibility in solutions was highlighted, allowing adaptation to various regulatory frameworks and customer requirements in different regions. The importance of developing pricing models that would make solutions accessible to smaller organizations, not just large market players, was also noted.
4. **Need for Ongoing Support and Development**: Several participants expressed a desire for the establishment of a permanent support mechanism after the project’s conclusion. This would include not only technical support but also continued updates to ensure solutions remain in step with the latest cybersecurity threats. The possibility of further joint development projects, involving both users and developers, was also suggested to pursue further improvements and adaptations of the solutions.
5. **Inclusion of a Broader Community**: Participants emphasized the importance of involving a wider range of stakeholders in future activities. This includes not only organizations within the energy industry but also regulators, research institutions, and other key players who can contribute to the development of a comprehensive ecosystem for cybersecurity in energy systems. They also suggested greater

participation in international initiatives and forums where CyberSEAS could showcase its achievements and exchange experiences with other projects.

These key aspects provide valuable guidance for future activities within the CyberSEAS project and beyond. The feedback will play a crucial role in shaping strategies for the implementation, marketing, and further development of solutions that will contribute to greater cybersecurity resilience in energy systems.

Time	**Presentation**	**Presenter**	
10:00-10.05	Welcome and introduction	Denis Caleta (ICS)	
10:05-10:25	Main steps in evolution of CyberSEAS project (approaching the last phase)	Paolo Roccetti (ENG)	
10:25-10:45	Playbooks and tools for standardized response, reporting, and coordination	Andrej Bregar (INF)	
10:45-11:05	From Labs to Real-World Testing: Deploying CyberSEAS Tools in Pilot Infrastructures	Luca Bianconi (STAM) Peter Krebelj (ELES)	
11:05-11:25	CyberSEAS tools for proactive security notifications	Andreas Papadakis (Synelixis)	
11:25-11:45	Heindall: Detect and monitoring of system vulnerabilities	Aitor Uribarren (Ikerlan)	
11:45-12:30	Market Interest Group (MIG) panel discussion. Pannel participants: 1. Anjos Nijk – Managing Director – European Network for Cyber Security 2. Olivier Voron – Digital Project Manager for Power Networks – RTE France 3. Gerhard Meindle – Business Development Manager – SWW Wunsiedel GmbH 4. Liviu Draguceanu – Digitalization Program Manager – EVRYO (former CEZ Romania) -	Mihai Mladin (CRENERG)	

	5. Mihai Truta – Director of Data Protection/ Information Security		
12:30-12:45	Discussion and proposals for the next meeting	All community members	
	Conclusion of the meeting		

Table 7: Program of 5th Stakeholder Community meeting

The fifth CyberSEAS Stakeholder Community meeting was a critical step in the project's timeline, particularly in terms of advancing the complex pilots. By focusing on real-world experiences and encouraging active participation from all members, we were able to gather essential feedback that will guide the next phases of the project and ensure that our efforts remain aligned with the needs of the broader EPES community.

CyberSEAS fourth Survey for Stakeholder community members – 29. MAY 2024

The survey conducted within the CyberSEAS Stakeholder Group, specifically targeting the Market Interest Group (MIG), was a pivotal step in ensuring that the project's technological developments and methodologies were aligned with the market's current demands and future needs. The focus of the survey was twofold: first, to assess the state and usability of existing technological solutions in the market, and second, to identify additional needs and gaps from the perspective of operational users. This dual approach was designed to provide a comprehensive understanding of where the market currently stands and where it needs to go, thereby helping to steer the project's final outputs in a direction that would ensure maximum relevance and impact.

Despite the fact that this particular survey received a lower response rate compared to previous ones, the depth and relevance of the responses were invaluable. The feedback highlighted critical areas where the solutions developed within CyberSEAS could fill existing gaps, offering new opportunities for technological advancement and market integration. These insights were particularly crucial as the project moved into its final stages, guiding the refinement of solutions and ensuring they met the specific, real-world needs of users within the EPES (Electric Power and Energy Systems) sector.

Moreover, the survey's findings played a significant role in shaping the strategic direction of Work Package 9 (WP9), "From Lab to Market." This work package was focused on transitioning the technologies developed during the project from the research and development phase into viable, market-ready products and services. The responses from the survey provided a clear indication of which aspects of the technology needed further development, customization, or validation to ensure they were not only technically sound but also commercially viable and aligned with user expectations.

In response to the survey, the project team took several critical steps. Firstly, they revisited the key technological innovations to address any identified gaps or concerns raised by the respondents. This included refining algorithms, enhancing user interfaces, and ensuring that the solutions could be seamlessly integrated into existing operational environments. Additionally, the project team worked closely with stakeholders to validate the practicality and usability of the technologies, conducting additional rounds of testing and feedback to fine-tune the solutions.

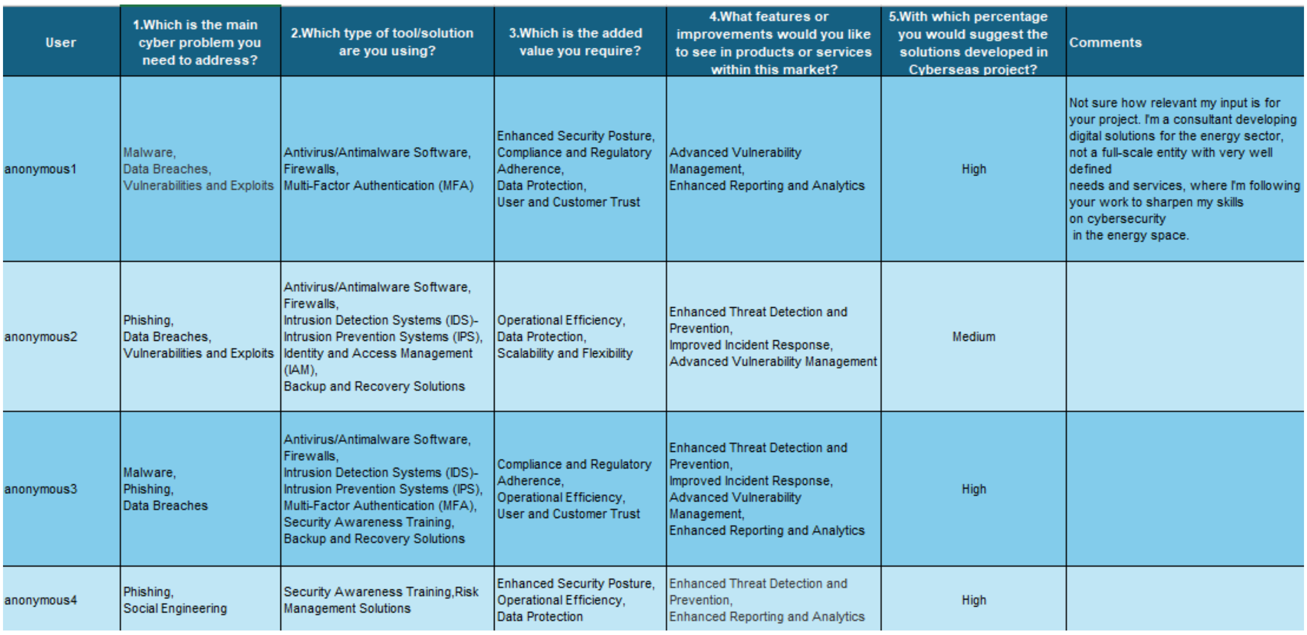
Furthermore, the survey underscored the importance of effective communication and collaboration between the project's developers and the end users. As a result, the CyberSEAS team intensified its efforts to engage with stakeholders, ensuring that their insights and feedback were continuously incorporated into the development process. This iterative approach helped to build trust and confidence among stakeholders, who saw their concerns and suggestions directly influencing the project's outcomes.

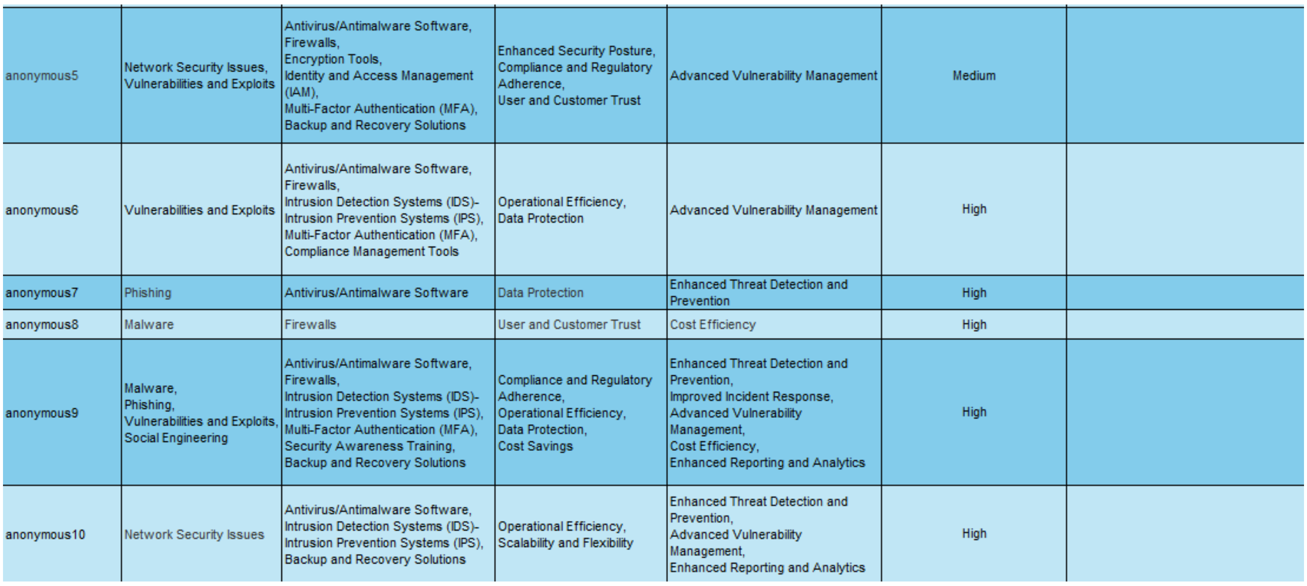
The feedback also led to the organization of additional targeted workshops and webinars, where stakeholders could engage directly with the technologies and provide real-time feedback. These sessions were instrumental in demonstrating the practical applications of the CyberSEAS solutions, showcasing their potential to address specific challenges within the EPES sector. By involving stakeholders in these hands-on experiences, the project was able to gather more nuanced insights, which were then used to make final adjustments to the technologies before they were brought to market.

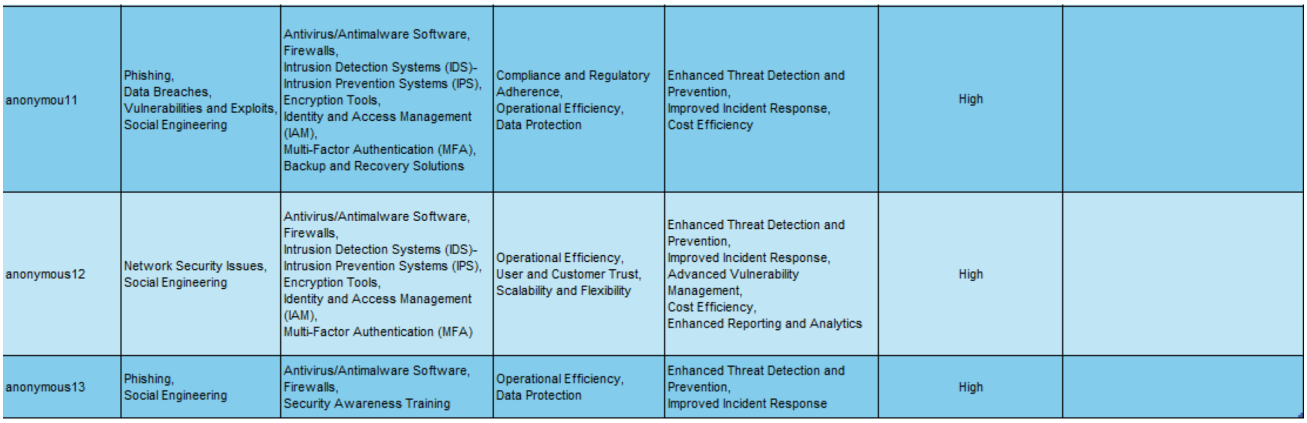
In the broader context, the survey highlighted the need for ongoing collaboration beyond the lifespan of the CyberSEAS project. Stakeholders expressed a strong interest in continuing the dialogue and exploring further opportunities for innovation and collaboration. This feedback prompted the project team to explore the formation of an ongoing stakeholder network or consortium that could continue to drive advancements in cybersecurity for energy systems, even after the official conclusion of the CyberSEAS project.

The survey conducted within the CyberSEAS Stakeholder Group, while initially modest in its response rate, had a profound impact on the project’s final phase. The feedback provided by the stakeholders was not only instrumental in refining the project’s outputs but also in ensuring that these outputs would have a lasting and meaningful impact on the market. The lessons learned and relationships built through this process have laid the groundwork for future collaboration, ensuring that the innovations developed within CyberSEAS will continue to evolve and adapt to meet the needs of the EPES sector in the years to come.

Here are the key feedback points we received from participants.







User	1.Which is the main cyber problem you need to address?	2.Which type of tool/solution are you using?	3.Which is the added value you require?	4.What features or improvements would you like to see in products or services within this market?	5.With which percentage you would suggest the solutions developed in Cyberseas project?	Comments
anonymous1	Malware, Data Breaches, Vulnerabilities and Exploits	Antivirus/Antimalware Software, Firewalls, Multi-Factor Authentication (MFA)	Enhanced Security Posture, Compliance and Regulatory Adherence, Data Protection, User and Customer Trust	Advanced Vulnerability Management, Enhanced Reporting and Analytics	High	Not sure how relevant my input is for your project. I'm a consultant developing digital solutions for the energy sector, not a full-scale entity with very well defined needs and services, where I'm following your work to sharpen my skills on cybersecurity in the energy space.
anonymous2	Phishing, Data Breaches, Vulnerabilities and Exploits	Antivirus/Antimalware Software, Firewalls, Intrusion Detection Systems (IDS)-Intrusion Prevention Systems (IPS), Identity and Access Management (IAM), Backup and Recovery Solutions	Operational Efficiency, Data Protection, Scalability and Flexibility	Enhanced Threat Detection and Prevention, Improved Incident Response, Advanced Vulnerability Management	Medium	
anonymous3	Malware, Phishing, Data Breaches	Antivirus/Antimalware Software, Firewalls, Intrusion Detection Systems (IDS)-Intrusion Prevention Systems (IPS), Multi-Factor Authentication (MFA), Security Awareness Training, Backup and Recovery Solutions	Compliance and Regulatory Adherence, Operational Efficiency, User and Customer Trust	Enhanced Threat Detection and Prevention, Improved Incident Response, Advanced Vulnerability Management, Enhanced Reporting and Analytics	High	
anonymous4	Phishing, Social Engineering	Security Awareness Training,Risk Management Solutions	Enhanced Security Posture, Operational Efficiency, Data Protection	Enhanced Threat Detection and Prevention, Enhanced Reporting and Analytics	High	
anonymous5	Network Security Issues, Vulnerabilities and Exploits	Antivirus/Antimalware Software, Firewalls, Encryption Tools, Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Backup and Recovery Solutions	Enhanced Security Posture, Compliance and Regulatory Adherence, User and Customer Trust	Advanced Vulnerability Management	Medium	
anonymous6	Vulnerabilities and Exploits	Antivirus/Antimalware Software, Firewalls, Intrusion Detection Systems (IDS)-Intrusion Prevention Systems (IPS), Multi-Factor Authentication (MFA), Compliance Management Tools	Operational Efficiency, Data Protection	Advanced Vulnerability Management	High	
anonymous7	Phishing	Antivirus/Antimalware Software	Data Protection	Enhanced Threat Detection and Prevention	High	
anonymous8	Malware	Firewalls	User and Customer Trust	Cost Efficiency	High	
anonymous9	Malware, Phishing, Vulnerabilities and Exploits, Social Engineering	Antivirus/Antimalware Software, Firewalls, Intrusion Detection Systems (IDS)-Intrusion Prevention Systems (IPS), Multi-Factor Authentication (MFA), Security Awareness Training, Backup and Recovery Solutions	Compliance and Regulatory Adherence, Operational Efficiency, Data Protection, Cost Savings	Enhanced Threat Detection and Prevention, Improved Incident Response, Advanced Vulnerability Management, Cost Efficiency, Enhanced Reporting and Analytics	High	
anonymous10	Network Security Issues	Antivirus/Antimalware Software, Intrusion Detection Systems (IDS)-Intrusion Prevention Systems (IPS), Backup and Recovery Solutions	Operational Efficiency, Scalability and Flexibility	Enhanced Threat Detection and Prevention, Advanced Vulnerability Management, Enhanced Reporting and Analytics	High	
anonymou11	Phishing, Data Breaches, Vulnerabilities and Exploits, Social Engineering	Antivirus/Antimalware Software, Firewalls, Intrusion Detection Systems (IDS)-Intrusion Prevention Systems (IPS), Encryption Tools, Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Backup and Recovery Solutions	Compliance and Regulatory Adherence, Operational Efficiency, Data Protection	Enhanced Threat Detection and Prevention, Improved Incident Response, Cost Efficiency	High	
anonymous12	Network Security Issues, Social Engineering	Antivirus/Antimalware Software, Firewalls, Intrusion Detection Systems (IDS)-Intrusion Prevention Systems (IPS), Encryption Tools, Identity and Access Management (IAM), Multi-Factor Authentication (MFA)	Operational Efficiency, User and Customer Trust, Scalability and Flexibility	Enhanced Threat Detection and Prevention, Improved Incident Response, Advanced Vulnerability Management, Cost Efficiency, Enhanced Reporting and Analytics	High	
anonymous13	Phishing, Social Engineering	Antivirus/Antimalware Software, Firewalls, Security Awareness Training	Operational Efficiency, Data Protection	Enhanced Threat Detection and Prevention, Improved Incident Response	High	

6th Stakeholder Community meeting – 12. SEP 2024 10:00-13:00 (on-line)

The final meeting of the CyberSEAS Stakeholder Community, conducted during the closing stages of the project's operational phase, was a pivotal event that aimed to consolidate and showcase the substantial progress made throughout the project's lifecycle. The session was meticulously organized to ensure that all members of the community had a comprehensive understanding of the final project outcomes. These included not only the practical achievements in implementing the project's objectives but also the significant technical advancements realized through the development of the proposed technologies.

During the meeting, a thorough presentation of the main conclusions was provided, particularly focusing on the execution and results of the pilot projects that had been carried out. These pilots were critical to validating the innovations developed during CyberSEAS and demonstrating their potential for real-world application. Given the sensitive nature of some pilot activities, particular care was taken to ensure that the content shared with the community was devoid of any confidential information or data that could pose a security risk. This approach safeguarded the interests of the pilot partners while allowing the broader community to benefit from the insights and lessons learned.

In addition to the technical presentations, the meeting also featured a significant discussion within the framework of the Market Interest Group (MIG). This segment was especially important, as it allowed stakeholders to explore and deliberate on the commercial and operational potential of the project's outcomes. The focus of the discussion was on identifying pathways to swiftly transition the technological and procedural advancements achieved through CyberSEAS into the operational practices of organizations within the EPES framework. The aim was to ensure that the innovations developed did not remain theoretical but were actively integrated into the practices of relevant industries, thereby enhancing cybersecurity resilience across the energy sector.

Time	Presentation	Presenter	
10:00-10.05	Welcome and introduction	Denis Caleta (ICS)	
10:05-10:25	Final steps in evolution of results in CyberSEAS project	Paolo Roccetti (ENG) – project coordinator	
10:25-10:45	Technical recap of the main achievements in project CyberSEAS	Luigi Romano (CINI) – technical coordinator	

10:45-11:50	From Labs to Real-World Testing: Deploying CyberSEAS Tools in Pilot Infrastructures (PILOT EXAMPLES) - Slovenian-Croatian pilot (20') - Romanian pilot (20') - Finish pilot (20')	Marjan Bogataj (OPER) – WP7 coordinator Paul Lacatus (CRE) Pekka Pietilä (ENERIM)	
11:50-12:35	Market Interest Group (MIG) final panel discussion. Pannel participants: Pannel participants: - Irina Clima - Director of Architecture, Cyber Audit, IT&C Governance and Cristian Barbulescu – Cybersecurity Expert – ELECTRICA SA - Marius-Iulian Rosu – Chief Information Security Officer – PPC Romania - Cosmin Ghita – Director of Digitalization and Innovation or Liviu Draguceanu – Digitalization Program Manager – EVRYO - Andrea Rocco Renna – Senior Vice-President – Comforte AG - Zahi Levi – Director BD Cyber Intelligence – Elbit Systems	Mihai Mladin (CRENERG)	
12:35-12:50	Discussion and proposals for the after CyberSEAS life time activities	All community members	
12:50	Conclusion of the meeting		

Table 8: Program of 6th Stakeholder Community meeting

Moreover, the meeting facilitated a critical discussion about the future of the CyberSEAS Stakeholder Community. Members recognized the importance of continuing their collaborative efforts beyond the project's official conclusion. The community had grown to include 101 members by this point, reflecting the broad interest and engagement in the project’s objectives. A dedicated administrator had been established to ensure the smooth operation and coordination of the group’s activities.

A key outcome of the discussion was the recognition of the need to seek out synergies with other related initiatives, with a particular focus on enhancing collaboration and avoiding duplication of efforts. One of the prominent proposals was to strengthen ties with the CyberEPES Cluster, a collective of projects focused on cybersecurity and energy grids. The CyberSEAS Stakeholder Community was seen as a natural foundation for expanding and deepening collaboration within this cluster. By aligning with the CyberEPES Cluster, the community could leverage a broader network of stakeholders, share resources, and amplify the impact of the innovations developed during CyberSEAS.

The meeting also addressed the community's ongoing commitment to promoting diversity and inclusion, particularly through initiatives like Women in Cyber. The project had consistently prioritized gender balance, and the final meeting provided an opportunity to highlight the contributions of female professionals in cybersecurity. Discussions were held on how to continue supporting and integrating initiatives like Women in Cyber into future activities, ensuring that the community remains a leader in promoting inclusive practices in the cybersecurity field.

The final meeting was not just a closure but a launching point for future endeavours. The comprehensive discussions and decisions made during this event set the stage for the CyberSEAS Stakeholder Community to continue its work, fostering collaboration, innovation, and practical application of cybersecurity advancements well beyond the formal conclusion of the CyberSEAS project. The proactive approach to finding synergies with related initiatives, like the CyberEPES Cluster, and the ongoing commitment to diversity and inclusion, demonstrated the community's dedication to creating a lasting impact in the field of cybersecurity and energy resilience.

5.2 Results and outcomes of clustering with relevant projects and initiatives

The project partners, within the coordination activities of WP8 "Fostering the Culture of Cyber-Resilient Energy Supply Chain" and specifically T8.1 "Stakeholder Community Building and Clustering with Other Relevant Projects and Initiatives," embarked on a comprehensive series of strategic networking and collaboration activities that significantly contributed to the project's overarching objectives. These activities were designed with meticulous planning, as laid out in D8.1, ensuring that every step taken was aligned with the project's goals and the broader context of cybersecurity within the EPES (Electric Power and Energy Systems) domain. The multidimensional networking framework was instrumental in achieving two key objectives. The first objective was to enhance the exchange of best practices, experiences, and to strengthen close cooperation among various stakeholders. This was not just limited to project partners but extended to a wider community, including other relevant projects, government bodies, and international organizations. The second objective focused on establishing and maintaining vital communication channels that enabled the effective presentation of the project's key results. These channels also played a crucial role in integrating these results into broader initiatives aimed at improving cybersecurity across the energy sector. To achieve these objectives, the project partners implemented a variety of targeted activities. These included organizing joint workshops, conferences, and webinars that facilitated knowledge sharing and collaboration across different sectors. Special attention was given to fostering relationships with other projects and initiatives that shared similar goals, thereby creating a synergistic environment where ideas and solutions could be exchanged freely. This approach not only amplified the impact of the CyberSEAS project but also contributed to a more cohesive and resilient energy supply chain on a global scale.

As part of WP8, the project also developed a collaborative model that was fully validated during the infrastructure pilots. This model was designed to enhance cooperation among individual operators within the energy supply chain and among operators of other EPES infrastructures. It was tested in real-world scenarios involving government institutions and municipalities, ensuring that the model was practical and effective in a variety of contexts. The validation process confirmed the model's applicability and value, making it a key component of the project's legacy. In addition to these collaborative efforts, the project also focused on integrating the lessons learned and the best practices identified during the project into broader policy and regulatory frameworks. This was particularly important for ensuring that the project's outcomes had a lasting impact on the cybersecurity landscape within the energy sector. By aligning the project's results with existing and emerging regulations, the project partners were able to contribute to the development of more robust and comprehensive cybersecurity policies that will benefit the entire energy supply chain.

The coordinated activities within WP8 and T8.1 of the CyberSEAS project have laid a solid foundation for the future of cybersecurity in the energy sector. Through strategic networking, community building, and the integration of best practices, the project has significantly advanced the state of cybersecurity within the EPES domain. The legacy of CyberSEAS will continue to influence the energy sector, providing valuable insights, tools, and frameworks that will help to ensure a secure and resilient energy supply chain for years to come.

Review of all organized activities:

DATE	**ACTIVITY**	**PARTNER PROJECT INITIATIVES**	**STATUS**
15/03/2022	Cyber EPES Cluster meeting with DG ENER and DG RIA representative (Important organization activities provided by CyberSEAS project. Use	Cyber EPES Cluster	Done

	also this opportunity to present CyberSEAS project.)		
27-29/04 2022	2nd ECSCI workshop (organization activities and CyberSEAS presentation) https://ec.europa.eu/newsroom/cipr/items/752425/en	ECSCI Cluster	Done
19 MAY 2022	Coordination meeting with Slovenian Corporate Security Association which result in first common collaboration with additional presenting CyberSEAS in International event "Days of Corporate Security 2022 31.MAY - 1. JUNE 2022	Slovenian Corporate Security Association and SE Europe Corporate Security Association	Done
MAR 2023	Meeting and presentation CyberSEAS project to ENTSO-E (ELES and HOPS were made a coordination with ENTSO-E (discussion about CyberSEAS was organize on Cyber Security Working Group (CSWG))	ENTSO-E	Done
JUN 2022	European Cybersecurity Organization (ECSO) (https://ecs-org.eu/) - Cyber Resilience CI WG (6.2 – Dr Roccetti is cochair – and cyber SEAS contact) – exchanging information about best practices exchanging information on regular WG meeting	ECSO	Done
NOV 2022	Meeting and presentation CyberSEAS project to MeliCERTes initiative (MeliCERT-es network meeting in framework of ENISA – Brno, Czech Republic) – CyberSEAS was presented by SI-CERT	MeliCERTes network	Done
JAN 2023	Workshop on legislative challenges in EPES environments (Supported by CyberSEAS)	Slovenian Corporate Security Association and SE Europe Corporate Security Association	Done

07/03/2023	Coordination meeting with ENISA representatives and discussing on topic "Achievements so far and plan for future activities«	ENISA	Done
12/05/2023	Coordination and cooperation activities cyberSEAS with e-FORT project https://cyberseas.eu/cyberseas-stakeholders-community-call-for-cooperation-with-other-projects-and-organizations/	e-FORT	Done
22/05/2023	CERT community meeting presentation of CyberSEAS project and discussion about follow up with transfer best practices form project to CERT community – contact organization was SI-CERT	ENISA / CERT community	Done
23-24/5/2023	Coordination with SE Europe Corporate Security Association (SECSA) (presentation and co-organization of panel in the international event „Days of Corporate Security 2023" which was held in Ljubljana	SECSA	Done
25/05/2023	CyberEPES Cluster meeting (exchanging best practices from CyberSEAS and searching additional possibilities for data sharing)	CyberEPES Cluster	Done
31/05/2023	Co-organizing CIGRE event with organizing special panel connected to CyberSEAS (Bled, Slovenia - 30MAY – 01JUN 2023 (coordinating partners ICS, OPERATO) https://www.ics-institut.si/en/news/presentation-of-the-cyberseas-project-at-an-important-event-of-the-international-organization-cigre-cired	CIGRE	Done
JUN 2023	Women In Cybersecurity Associations – SI CERT (Mrs. Maja Horvat) – presenting CyberSEAS and discussing about possible next step cooperation	Women4Cyber initiative	Done
JUN 2023	The Italian businesses Trust-IT Srl and Engineering Ingegneria Informatica S.p.A (ENG) and cyberSEAS coordinator have	Trust-IT	Done

	signed a Memorandum of Understanding (MoU) to further strengthen their partnership and collaboration within the context of EU Funded Projects. https://cyberseas.eu/memorandum-of-understanding-mou-is-signed-between-ingegneria-informatica-s-p-a-eng-and-trust-it-srl/		
JUN 2023	European Cybersecurity Organization (ECSO) (https://ecs-org.eu/) - Cyber Resilience CI WG (6.2 – Dr Roccetti is cochair – and cyber SEAS contact) – exchanging information about best practices on regular WG meeting	ECSO	Done
JUN 2023	Contribution to FIWARE (data model) security (co-organizing FIWARE bootcamp 5-9. JUNE 2023 and participate at Global Summit (Vienna 12-13. JUNE 2023) (coordinating partner CINI)	FIWARE	Done
AUG 2023	Prepared and signed Memorandum of Understanding (MoU) between EU project ICT Standardization Observatory and Support Facility in Europe (StandICT)(www.standict.eu), and CyberSEAS https://cyberseas.eu/post_mou-signed-between-standict-eu-cyberseas-project_aug23/	StandICT	Done
20/09/2023	The EU-CIP project and ECSCI cluster co-organized the "1st Annual Conference on Critical Infrastructure Resilience: Reinventing European Resilience, 20-21 September 2023 (ECSCI workshop is scheduled on 20 September 14:00-17:30) (organization activities and CyberSEAS presentation) https://www.eucip.eu/2023/09/29/1st-eu-cip-annual-conference-promotes-reinventing-resilience-for-european-critical-infrastructures/	EU-CIP and ECSCI cluster	Done

27/11/2023	The State Council of the Republic of Slovenia held a national consultation entitled "Resilience and business continuity of key organizations - an imperative of modern society" in the co-organization of the State Council, the Institute for Corporate Security Studies (ICS) and the Slovenian Association for Corporate Security. (CyberSEAS best approaches and practices was presented and discussed) https://www.ics-institut.si/en/news/presentation-of-cyberseas-project-at-the-national-consultation-of-the-state-council	State Council of the Republic of Slovenia and Slovenian Association for Corporate Security	Done
05/12/2023	Organization ECSCI international on-line event „Standardisation and policy making for increasing resilience of Cis“– (ATLANTIS, SUNRISE, CyberSEAS, PRECINCT) https://www.ics-institut.si/en/news/ecsci-online-workshop-entitled-collaborative-standardization-and-policy-making-for-greater-ci-resilience-in-europe	ECSCI cluster	Done
18/01/2024	CyberEPES Cluster meeting (discussion about possible transformation the new knowledge form CyberSEAS to other projects in cluster)	CyberEPES Cluster	Done
15/02/2024	Standardization focus meeting with ICT Standardization Observatory and Support Facility in Europe (StandICT) (www.standict.eu), and CyberSEAS	StandICT	Done
01/03/2024	Presentation of CyberSEAS project in RDIC Innovation Fridays (presentation of the evolution steps in project CyberSEAS and discussion about possible implementation of new solutions and processes)	ENTSO-E	Done
MAR 2024	Webinar »Unpacking cyber-resilience for EPES with NIS2 (Woman's perspective)« organized in cooperation with the CyberSEAS project and the Slovenian delegation of Women4Cyber (21 March 2024)	Women4Cyber initiative	Done

	https://cyberseas.eu/watch-now-webinar-unpacking-cyber-resilience-for-epes-with-nis2-womans-perspective/		
APR2024	International conference within the SE Europe Corporate Security Association Presentation of outcomes and best practices of CyberSEAS	SEECSA	Done
13/05/2024	Coordination meeting with Slovenian Corporate Security Association which result in third common collaboration with presenting CyberSEAS best practices and possible innovations for operational environment in international event "Days of Corporate Security 2024	Slovenian Corporate Security Association and SE Europe Corporate Security Association	Done
JUN 2024	Prepare White Paper Energy Sector - Digital security issues for critical infrastructures – Focus on the Electricity Sector. Participating author form CyberSEAS Dr. Luigi Rommano	EU-CIP	Done
SEP 2024	BRIDGE Business Models WG (Coordinating and exchanging best practices with Cyber SEAS project) coordinating partners CRE, RTWH, ENG (Brussels meeting)	BRIDGE	Done

Table 9: Review of all organized collaborative activities

In the table above, we have provided a chronological overview of all the collaboration, coordination, presentations, exchange of best practices, and joint organization activities conducted in partnership with significant initiatives and projects that have a profound impact on the European Power and Energy Systems (EPES). These activities are characterized by their strategic distribution and targeted focus, ensuring they reached all levels, from national to international arenas.

Our collaborative efforts encompassed a wide range of activities. On one hand, they involved the pursuit of policy and legislative solutions, which are crucial for shaping a robust cybersecurity framework within EPES. On the other hand, we also concentrated on standardization efforts, ensuring that the best practices developed within the project were effectively transferred to partner initiatives. This exchange of information extended to the technological solutions and innovative process approaches within the EPES sector, demonstrating our commitment to fostering a holistic understanding of cybersecurity challenges and solutions.

Importantly, our collaboration was not confined to the EPES domain alone. We actively sought to engage with the broader cybersecurity landscape, particularly in the context of critical infrastructure and essential service providers. This approach allowed us to address a wider array of challenges and opportunities, reinforcing the interconnected nature of cybersecurity across various sectors.

Moreover, we placed significant emphasis on specific areas of concern that have garnered substantial attention within the European Union, such as the inclusion and empowerment of women in cybersecurity. Recognizing the vital role that diversity plays in enhancing the cybersecurity field, we worked closely with female experts within our project, dedicating considerable effort to transferring insights and experiences to the broader Women4Cyber community. This initiative not only aimed to support the professional growth of women in cybersecurity but also to enrich the field with diverse perspectives and expertise.

In addition to our primary collaborative efforts, we also initiated targeted outreach and engagement activities with key stakeholders, ensuring that our project's findings and innovations were effectively communicated and adopted within relevant communities. This included organizing specialized workshops, webinars, and discussion forums where we could directly interact with stakeholders, gather valuable feedback, and refine our approaches based on real-world needs and challenges.

By strategically engaging with a broad spectrum of stakeholders—ranging from policymakers to industry experts and academic researchers—we aimed to create a resilient and responsive network that could drive meaningful advancements in the cybersecurity of EPES. The insights and lessons learned from these interactions were not only instrumental in guiding the project to successful outcomes but also in laying the groundwork for ongoing collaboration and innovation beyond the project's lifespan.

Furthermore, our efforts to integrate the experiences and knowledge gained into the Women4Cyber community serve as a testament to our commitment to fostering an inclusive cybersecurity environment. By sharing our project's successes and challenges with this community, we contributed to the broader goal of achieving gender equity in cybersecurity, while also ensuring that the solutions we developed are adaptable and relevant to a diverse workforce.

This comprehensive approach to collaboration, outreach, and inclusion underscores the multifaceted nature of the CyberSEAS project's impact. It highlights our dedication to not only addressing immediate cybersecurity challenges within EPES but also to contributing to the long-term resilience and sustainability of the sector by engaging with a broad and diverse set of stakeholders.

Iniciative	**Number of Activities**
European Cluster for Securing Critical Infrastructure (ECSCI)	3
Cybersecurity Innovation Cluster for EPES	4

FIWARE	2
ENISA/ MeliCERTes network	2
ENISA	1
CIGRE/CIRED	1
SE Europe Corporate Security Association	5
Initiative Trust-IT	1
Initiative StandICT	2
e-FORT project	1
European Network of Transmission System Operators for Electricity (ENTSO-E)	2
Women in Cyber Security	2
European Cybersecurity Organization (ECSO)	2
BRIDGE Cluster	1
EU-CIP (https://www.eucip.eu/) initiative	2
Total	**31 (activities)** **15 (Initiatives)**

Table 10: Summary of all organized collaborative activities

In the table provided, we have gathered and organized a detailed overview of the activities carried out in connection with each specific initiative or project. This overview includes a breakdown of individual activities, followed by a cumulative total for each initiative, allowing for a clear and concise presentation of the overall efforts made.

This detailed record serves multiple purposes. Firstly, it provides transparency and accountability by documenting the breadth and depth of our engagements. By quantifying the activities associated with each initiative, we can better assess the impact and effectiveness of our collaboration efforts.

Secondly, the table highlights the strategic importance of our collaborations. The cumulative totals offer a snapshot of how intensively we have engaged with each initiative, illustrating our focused efforts to build strong, meaningful partnerships. These figures are not merely statistical; they represent our proactive approach to ensuring that our collaborations are not just nominal but deeply integrated into the broader goals of the CyberSEAS project.

Additionally, by exceeding the initial indicators for achieving our objectives, we underscore the success of our strategic planning and execution. The numbers reflect more than just activities—they signify our dedication to surpassing expectations, driving meaningful change, and contributing significantly to the advancement of cybersecurity within the EPES domain.

This comprehensive summary also underscores the diversity and range of our collaborative efforts. It demonstrates that our engagement was not confined to a narrow scope but rather spanned across various levels, from local to international contexts, addressing different facets of cybersecurity. By documenting and analysing these efforts, we not only validate the success of our current initiatives but also lay a strong foundation for future collaborations, ensuring that the momentum we have built continues to drive progress long after the project’s official end.

Moreover, the data captured in this table is instrumental in guiding our future strategic directions. It helps identify areas where we have excelled, as well as opportunities for further improvement and expansion. This allows us to refine our approach, ensuring that we continue to set ambitious yet achievable goals in our ongoing efforts to enhance cybersecurity resilience across the EPES sector and beyond. Finally, this detailed tracking of activities also serves as a powerful communication tool. It allows us to effectively convey the scope and impact of our efforts to stakeholders, partners, and the broader community, reinforcing the value of our contributions and encouraging continued support and engagement in our future endeavours.

5.2.1 Key Performace Indicators (KPI)

At the outset of the CyberSEAS project, Key Performance Indicators (KPIs) were clearly established for all activities related to Task T8.1, which focused on stakeholder community building and clustering with other relevant projects and initiatives. Among the established KPIs, some are linked to multiple work packages (WPs), with the activities carried out under the aforementioned task being only part of the efforts to achieve the final set objectives.

The following table outlines the KPIs that were directly connected to the work within WP8, and more specifically to Task T8.1.

	ACTIONS	KPI's	Time	Results
1.	Working groups involvement, establishment links with initiatives, thematic network on Critical Energy Infrastructure Protection, ect.	Target: 15 references to work produced in CyberSEAS across at least 5 initiatives	M12-M36	31 (activities) 15 (Initiatives)
2.	CyberSEAS Stakeholder Community	100 members	M01-M36	101 members

Table 11: Summary of KPI's focused on WP8

The following table presents the results where the outcomes from WP2, WP3, WP4, WP5, and WP6 were transformed through established channels for collaboration and the exchange of experiences with the external professional EPES community.

	ACTIONS	KPI's	Time	Results
1.	Within the CyberSEAS Stakeholder Community, seven meetings were organized where specific technological and process solutions from the CyberSEAS project were presented. Four evaluation surveys were conducted, providing direct feedback from the energy stakeholders involved in the CyberSEAS Stakeholder Community.	Target: 15 external energy grid operators using **CyberSEAS risk self-assessment** and rating them as superior to currently available offerings	M12-M36	16 participants from external grid operators
2.	Within the CyberSEAS Stakeholder Community, seven meetings were organized	Target: 50 external energy stakeholders taking up the	M12-M36	72 external energy stakeholders

	where specific technological and process solutions from the CyberSEAS project were presented. Four evaluation surveys were conducted, providing direct feedback from the energy stakeholders involved in the CyberSEAS Stakeholder Community.	**CyberSEAS governance and cooperation support** to actively participate to information exchange		participated (in total on all meetings)

Table 12: Summary of KPI's where WP8 provided a collaborative framework

Through the presented KPIs, the CyberSEAS project has demonstrated a broad range of activities that consistently ensured an effective process of community building and clustering with relevant target projects and initiatives throughout the project's duration. Importantly, these activities were not only focused on the project's timeline but were also strategically aimed at extending their impact beyond the project's completion. This forward-looking approach ensures that the established networks, collaborations, and practices will continue to benefit the EPES community and the broader field of cybersecurity in the energy sector, even after the project's official end.

6 Conclusion (UPDATED)

An updated version of deliverable D8.2 focused on reporting the results and lessons learned as well as highlighting major outcomes of the planned actions.

This deliverable defines the strategy and activities for creation CyberSEAS Stakeholder Community and clustering with other relevant projects and initiatives. The report helps us understand implementation of efficient steps for creation of a Stakeholder Community and indication of different dissemination channels for exchanging Collective Intelligence. The report has gathered substantial contributions from leading partners in this area. The process of creation of Stakeholder Community has been extensive after the detailed analyses conducted and preparation of a draft plan of evolution of the CyberSEAS Stakeholder Community and analysing possible options for clustering with different existing initiatives and projects. The creation of Stakeholder Community and clustering opportunities are closely connected with developing strategy and activities in dissemination in the CyberSEAS project. This is important due to close collaboration with scientific and professional communities in EPES area. Further synergies have been even more visible in joint work of these processes including management and exploitation.

The report also brings the detail activities which have been made on the base of creation Stakeholder Community plan provided in D8.1. On a base of analysis of the relevant organizational approaches, communication channels and the most important set the analysis of the existing and operational clusters and projects. The focus in the period cover from D8.2 is focus in fostering all necessary activities after creation of the Stakeholder Community and accelerating and carrying out the proper activities regarding exchanging best practices, latest technological and procedural achievements and new knowledge.

We can conclude that there was a substantial effort put in operating CyberSEAS Stakeholder Community and clustering with relevant indicatives and projects. There is also a strong base for further after project lifecycle period additional development of the Stakeholder Community and clustering activities. CyberSEAS project partners together with involved organizations and members from EPES area identified and operationalized substantial number of different collaborative activities which brings additional value for the project per se but also for collaborating partner organizations. Focus of this collaboration have been directed primarily on opportunities in the wide rand of different topics related to physical and cyber protection of EPES environments. The complexity of Collective Intelligence processes in CyberSEAS showed a wider view on processes connected with Critical Infrastructure Protection in broader sense. Technical CyberSEAS partners also searched new opportunities for dissemination of their new technical solutions in the period after the CyberSEAS lifecycle through the Stakeholder Community.

The work on this task has provided positive feedback about the executed clustering process and organized Stakeholder Community efforts. It is also good fundamental base that community members will continue in the mission of strengthening the organizational and procedural aspects of the Stakeholder Community and scaling up the communication channels for the exchanging process in the area of providing EPES security.

7 References

[1] EPRS | European Parliamentary Research Service, p. 5, https://www.researchgate.net/publication/340350926_Collective_intelligence_at_EU_level_Social_and_democratic_dimensions

[2] EPRS | European Parliamentary Research Service, p. 6, https://www.researchgate.net/publication/340350926_Collective_intelligence_at_EU_level_Social_and_democratic_dimensions

[3] Jiwat Ram (2019). Using Collective Intelligence in PM: Time to take the leap? https://www.ipma.world/using-collective-intelligence-in-pm-time-to-take-the-leap/

[4] Kleopatra Alamantariotou, Athina Lazakidou, Anastasia Topalidou, Georgia Kontosorou, Maria Tsouri, Michaela Michel-Schuldt and Charalambos Samantzis (2014). Collective Intelligence for Knowledge Building and Research in Communities of Practice and Virtual Learning Environments: A Project Experience. *International Journal of Health Research and Innovation, vol. 2, no. 1, 2014, 51-64 ISSN: 2051-5057 (print version), 2051-5065 (online) Scienpress Ltd, 2014*

[5] https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf

[6] Regulation No. 2019/941 https://eur-lex.europa.eu/eli/reg/2019/941/oj

[7] https://www.h2020-bridge.eu/working-groups/data-management/

[8] https://www.etip-snet.eu/

[9] https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf

[10] https://www.ee-isac.eu/

[11] https://mcusercontent.com/fac8062360203f4bc7e2b068e/files/1fa674ce-42af-44a8-81d9-7a90bc827312/EE_ISAC_Incident_Response_White_Paper_final.pdf

[12] https://www.etip-snet.eu/

[13] https://www.ee-isac.eu/

[14] https://www.prnewswire.com/news-releases/elering-grid-operators-to-establish-energy-data-accessalliance-to-revolutionize-european-energy-market-300966098.html#:~:text=Energy%20Data%20Access%20Alliance%20aim,full%20control%20over%20their%20data.

[15] Directive (EU) 2016/1148, https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[16] Directive (EU) 2022/2555 https://eur-lex.europa.eu/eli/dir/2022/2555